(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年3 月21 日 (21.03.2002)

PCT

(10) 国際公開番号
WO 02/23903 A1

(51) 国際特許分類[7]: H04N 7/16

(21) 国際出願番号: PCT/JP01/07924

(22) 国際出願日: 2001 年9 月12 日 (12.09.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-277177 2000 年9 月12 日 (12.09.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 浅津英樹 (ASADU, Hideki) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 弁理士 松隈秀盛(MATSUKUMA, Hidemori); 〒160-0023 東京都新宿区西新宿1丁目8番1号 新宿ビル Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

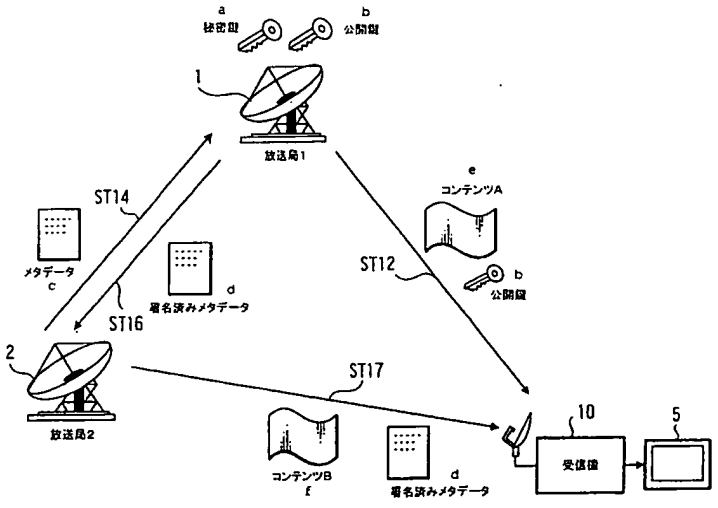
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: INFORMATION PROCESSING DEVICE, ELECTRONIC DEVICE, INFORMATION PROCESSING METHOD, AND MEDIUM

(54) 発明の名称: 情報処理装置、電子機器、情報処理方法及び媒体



(57) Abstract: When a first content previously distributed is referred to in relation to a second content, the limit on the use of the first content effectively functions. A secret key and a public key are generated for the first content, and the first content to which the public

[続葉有]

WO 02/23903 A1

key is added is transmitted. When a second content for which the user wants to refer to the second content is generated, the manager managing the first content is requested to sign predetermined data added to the second content by means of the secret key generated when the first content is broadcast. After the signature, the second content to which the signed predetermined data is added is transmitted. On the receiving side, collation of the signature on the predetermined data is performed by means of the public key added to the first content. If the collation succeeds, the stored first content is subjected to a predetermined processing according to the instruction of the second content and outputted.

(57) 要約:

過去に配信された第１のコンテンツを、第２のコンテンツが参照する処理を行う際に、その第１のコンテンツの利用制限が有効に機能にするようにする。このために、第１のコンテンツに対して、秘密鍵と公開鍵を生成させ、その公開鍵を付加して、第１のコンテンツを送信し、その後、第１のコンテンツを参照したい第２のコンテンツが発生したとき、第２のコンテンツに付加される所定データに対して、第１のコンテンツ放送時に生成させた秘密鍵での署名を、第１のコンテンツの管理者に要求し、その署名が行われたとき、その署名された所定データが付加された第２のコンテンツを送信する。受信側では、第１のコンテンツに付加された公開鍵を使用して、第２のコンテンツに付加された所定データの署名を照合する処理を行い、照合に成功したとき、第２のコンテンツの指示に基づいて、蓄積された第１のコンテンツに所定の加工を施して出力する。

明　　細　　書

情報処理装置、電子機器、情報処理方法及び媒体

技術分野

本発明は、例えばテレビジョン放送の番組などのコンテンツを送信して受信する情報処理方法と、その情報処理方法を適用した情報処理装置及び電子機器、並びに情報処理方法が実行されるプログラムが格納又は伝送される媒体に関する。

背景技術

従来、テレビジョン放送は、その放送を受信したときに、その放送を受信した受信機に接続（又は一体化）された受像機で、リアルタイムにその放送番組を視聴するか、或いはビデオテープレコーダなどの記録再生装置で、その番組を一旦記録し、その記録されたテープなどを任意の時間に再生させて視聴することが行われていた。

いずれの場合でも、従来は基本的には受信した番組をそのまま視聴するだけであり、例えばビデオテープに記録させて再生する際に、早送りなどを送って一部を飛ばすことができる程度であった。

これに対して、近年、ディスク（ハードディスク，光ディスク，光磁気ディスクなど）を媒体とした記録再生装置の性能の向上やコストの低下に伴って、放送信号の受信機に、ディスク記録再生装置を内蔵させて、受信した放送番組のデータを内蔵されたディスク記録再生装置に記録させておき、その記録された番組データをユーザが任意の時間に再生させることが可能になりつつある。

この場合、ディスク記録再生装置の場合には、記録された任意

のデータへのアクセスが容易であるため、ユーザの操作に基づいて、任意の形態で再生させるようにすることも可能である。

一方、放送局からデジタルデータで番組データが伝送されるいわゆるデジタル放送の場合には、番組内容そのもののデータであるコンテンツデータの他に、各種データを付加して伝送することが可能であり、その付加データを使用して、デジタル記録再生装置に記録されたコンテンツデータの再生形態を指示するようなことも考えられている。

例えば、ある特定の番組（コンテンツＡとする）が放送されたとき、そのコンテンツＡをあるユーザの受信機に内蔵された記録装置で記録させたとする。その後、別の番組（コンテンツＢとする）が放送されたときに、コンテンツＡが受信機内に蓄積されたユーザに対しては、コンテンツＡの一部の画像などを、コンテンツＢの視聴時に参照させることを指示するデータを放送局側から送り、そのデータに基づいて、各ユーザの受像機では、例えばコンテンツＡの画像とコンテンツＢの画像とを合成して表示させることを実現させることが提案されている。このような放送局側から送られるデータに基づいた指示で、表示形態などが設定される場合には、基本的にはユーザは特別な操作を必要としない。

このようにすることで、過去に放送したコンテンツを有効活用した新たなコンテンツを生成させることが可能になり、テレビジョン放送などの新たな利用形態を作り上げることができる。

しかしながら、過去に放送されたコンテンツＡを、別のコンテンツＢの視聴時に加工利用するようにすること、コンテンツＡの製作者や放送業者の権利を侵害するおそれがある。このため、このような過去の蓄積されたコンテンツを利用する場合には、何らかの制限を設けて、コンテンツＡの著作権者などを侵害しないような処理が必要である。

既に提案されている過去のコンテンツの利用制限処理としては、例えば、コンテンツＡを放送する際に、そのコンテンツＡを参照することを許可したコンテンツのリスト（アクセスコントロールリスト）のデータを配信することが考えられている。ところが、コンテンツＡを放送した時点で、将来そのコンテンツＡが他のコンテンツでどのように利用されるのかを予測するのは困難であり、コンテンツＡを配信する際に、参照可能なコンテンツの完全なリストのデータを作成するのは困難である問題がある。

このためには、コンテンツＡのアクセスコントロールリストを将来に渡って更新させることも考えられるが、過去に配信された個々のコンテンツのアクセスコントロールリストを個別に管理させて更新させることは、管理コストなどを考えると現実的ではない。

発明の開示

本発明は、過去に配信されたコンテンツを、別のコンテンツが参照する処理を行う際に、その過去のコンテンツの利用制限が有効に機能にするようにすることを目的とする。

第１の発明は、ネットワークを介して情報の授受を行う情報処理装置において、

上記第１のコンテンツに対して、秘密鍵と公開鍵を生成させて管理する鍵管理手段と、

上記鍵管理手段で管理する公開鍵を付加して、上記第１のコンテンツを送信する第１の送信手段と、

上記第２のコンテンツに付加される所定データに対して、上記鍵管理手段が管理する秘密鍵での電子署名を要求し、その電子署名された所定データが付加された上記第２のコンテンツを送信する第２の送信手段とを備えたものである。

このようにしたことによって、第１のコンテンツの管理者に参照することが許可された場合にだけ、正しい署名が行われた所定データが第２のコンテンツに付加されるので、第１のコンテンツを蓄積した各受信者側の設備では、第１のコンテンツを参照しても良いと許可されたコンテンツを受信したときだけ、自動的に別のコンテンツが第１のコンテンツを参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

第２の発明は、第１の発明の情報処理装置において、

上記鍵管理手段は、上記第２の送信手段からの電子署名要求時に、上記第２のコンテンツによる第１のコンテンツの参照が、第１のコンテンツの所定の権利を侵害しないと判断したときだけ、上記所定データへの電子署名を実行するようにしたものである。

このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部を利用した別のコンテンツを作成して視聴させることができるようになる。

第３の発明は、ネットワークを介して情報の授受を行う情報処理装置において、

第１のコンテンツと、第１のコンテンツに関連する所定データとを、第２のコンテンツに適用される秘密鍵を用いて上記所定データに電子署名を行った電子署名データに組み合わせて送信する第１の送信手段を備えたものである。このようにしたことによって、例えば第１のコンテンツを送信する場合に、既に放送などが行われた第２のコンテンツを利用を許可するデータを良好に送信できるようになる。

第４の発明は、第３の発明の情報処理装置において、

上記電子署名データを取得する電子署名データ取得手段を有するものである。このようにしたことによって、例えば、離れた場所で電子署名された電子署名データを取得できるようになる。

第５の発明は、第３の発明の情報処理装置において、

上記秘密鍵を使用して電子署名が行われる上記所定データは、上記第２のコンテンツの参照命令を含むようにしたものである。このようにしたことによって、例えば、第１のコンテンツを出力させる際に、必ず第２のコンテンツを参照するようになり、第１のコンテンツだけが出力されるようなことを防止できる。

第６の発明は、第５の発明の情報処理装置において、

上記所定データは、第１のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有するものである。このようにしたことによって、第１のコンテンツの第２のコンテンツへの挿入が、決められた位置に行われるようになる。

第７の発明は、

コンテンツデータを受信する受信手段と、

上記受信手段が受信したコンテンツを蓄積するコンテンツ蓄積手段と、

上記コンテンツ蓄積手段に蓄積された第１のコンテンツに付加された鍵データを使用して、上記受信手段が受信した第２のコンテンツに付加された所定データの電子署名を照合する照合手段と、

上記照合手段での照合が成功したとき、上記コンテンツ蓄積手段に蓄積された第１のコンテンツを、上記第２のコンテンツでの指示に基づいて加工するコンテンツ加工手段と、

上記コンテンツ加工手段で加工されたコンテンツを出力するコンテンツ出力手段とを備えた電子機器としたものである。このよ

うにしたことによって、第１のコンテンツを参照しても良いと許可されたコンテンツを受信したときだけ、自動的に別のコンテンツが第１のコンテンツを参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

第８の発明は、第７の発明の電子機器において、

上記コンテンツ加工手段での加工は、上記第１のコンテンツによる画像又は音声と上記第２のコンテンツによる画像又は音声を合成する処理としたものである。このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの画像又は音声と、後から送信されたコンテンツとの画像又は音声とを合成させて視聴又は聴取させることができるようになる。

第９の発明は、第７の発明の電子機器において、

上記コンテンツ加工手段での加工は、上記第１のコンテンツによる画像又は音声の一部を、上記第２のコンテンツによる画像又は音声に置き替える処理としたものである。このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部の画像や音声などを最新のデータに置き替えて視聴させることができるようになる。

第１０の発明は、第７の発明の電子機器において、

上記コンテンツ加工手段での加工は、上記第１のコンテンツによる画像又は音声を、第２のコンテンツによる指示で編集する処理としたものである。このようにしたことによって、過去のコンテンツの管理者に許可された場合にだけ、例えば、過去の特定のコンテンツのハイライトシーンだけを表示させるようなことが可能になる。

第１１の発明は、ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する電子機器において、

第１のコンテンツと、上記第１のコンテンツに関連する第１の所定データと、第２のコンテンツに適用される秘密鍵を上記第１の所定データに用い生成された電子署名データとの組み合わせデータを受信する第１の受信手段を有するものである。このようにしたことによって、例えば第１のコンテンツを受信した場合に、既に放送などが行われた第２のコンテンツを利用を許可するデータを良好に受信できるようになる。

第１２の発明は、第１１の発明の電子機器において、

上記秘密鍵を使用して電子署名が行われる上記第１の所定データは、第２のコンテンツの参照命令を含むものである。このようにしたことによって、第１のコンテンツを受信したとき、確実に第２のコンテンツを参照するようになる。

第１３の発明は、第１２の発明の電子機器において、

上記第１の所定データは、第１のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有するものである。このようにしたことによって、第１のコンテンツの第２のコンテンツへの挿入が、決められた位置に行われるようになる。

第１４の発明は、第１１の発明の電子機器において、

第２のコンテンツと上記秘密鍵に対応する公開鍵とを受信する第２の受信手段と、

受信された上記第２のコンテンツと上記公開鍵を記憶する記憶手段とを有するものである。このようにしたことによって、記憶手段に記憶された第２のコンテンツと公開鍵とを利用して処理できるようになる。

第１５の発明は、第１４の発明の電子機器において、

上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成する復号化手段と、

上記第１の所定データを所定のアルゴリズムに基づいて第２の所定データに変換するデータ変換手段と、

上記復号化手段により生成された上記復号化データと、上記データ変換手段により変換された上記第２の所定データとを照合する照合手段とを有するものである。このようにしたことによって、照合で一致した場合にだけ、記憶した第２のコンテンツを利用できるようになる。

第１６の発明は、第１５の発明の電子機器において、

上記照合手段の照合結果が一致した場合、上記第１の所定データに基づき上記記憶手段に記憶された第２のコンテンツを所定のタイミングで参照する参照手段とを有するものである。このようにしたことによって、第２のコンテンツを参照することが、確実に行えるようになる。

第１７の発明は、第１のコンテンツと、この第１のコンテンツを参照する第２のコンテンツを処理する情報処理方法において、

上記第１のコンテンツに対して、秘密鍵と公開鍵を生成させ、

上記生成された公開鍵を付加して、上記第１のコンテンツを送信し、

上記第２のコンテンツに付加される所定データに対して、上記秘密鍵での電子署名を要求し、

上記電子署名された所定データが付加された上記第２のコンテンツを送信するものである。このようにしたことによって、第１のコンテンツの管理者に参照することが許可された場合にだけ、正しい署名が行われた所定データが第２のコンテンツに付加されるので、第１のコンテンツを蓄積した各受信者側の設備では、第１のコンテンツを参照しても良いと許可されたコンテンツを受信

したときだけ、自動的に別のコンテンツが第１のコンテンツを参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

第１８の発明は、第１７の発明の情報処理方法において、

送信される上記第１のコンテンツを受信して蓄積した状態で、送信される上記第２のコンテンツを受信した場合に、蓄積された第１のコンテンツに付加された公開鍵を使用して、上記所定データの電子署名を照合し、

その照合に成功したとき、受信した上記第２のコンテンツの指示に基づいて、上記蓄積された第１のコンテンツに所定の加工を施して出力するものである。このようにしたことによって、過去に受信した第１のコンテンツを利用して第２のコンテンツを出力させることが、良好に行える。

第１９の発明は、ネットワークを介して情報の授受を行う情報処理方法において、

第１のコンテンツと、第１のコンテンツに関連する所定データとを送信する場合に、

上記第１のコンテンツとは別の第２のコンテンツに適用される秘密鍵を用いて、上記所定データに電子署名を行い、

その電子署名された電子署名データを上記所定データに組み合わせて送信するものである。このようにしたことによって、例えば第１のコンテンツを送信する場合に、既に放送などが行われた第２のコンテンツを利用を許可するデータを良好に送信できるようになる。

第２０の発明は、第１９の発明の情報処理方法において、

上記秘密鍵を用いた電子署名を、上記第２のコンテンツ又は上記秘密鍵を管理する側に依頼し、その依頼に基づいて得られた電

子署名データを、上記所定データに組み合わせるようにしたものである。このようにしたことによって、例えば、離れた場所で電子署名された電子署名データを取得できるようになる。

第２１の発明は、第１９の発明の情報処理方法において、

上記秘密鍵を使用して電子署名が行われる上記所定データは、上記第２のコンテンツの参照命令を含むようにしたものである。このようにしたことによって、例えば、第１のコンテンツを出力させる際に、必ず第２のコンテンツを参照するようになり、第１のコンテンツだけを出力させるようなことを防止できる。

第２２の発明は、第２１の発明の情報処理方法において、

上記所定データは、第１のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有するものである。このようにしたことによって、第１のコンテンツの第２のコンテンツへの挿入が、決められた位置に行われるようになる。

第２３の発明は、ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する情報処理方法において、

第１のコンテンツを記録するとき、上記第１のコンテンツに関連する第１の所定データと、既に記録された第２のコンテンツに適用される秘密鍵を上記第１の所定データに用い生成された電子署名データとを記録するものである。このようにしたことによって、第２のコンテンツを参照することを指示するデータを良好に記録できるようになる。

第２４の発明は、第２３の発明の情報処理方法において、

上記秘密鍵を使用して電子署名が行われる上記第１の所定データは、第２のコンテンツの参照命令を含むようにしたものである。このようにしたことによって、例えば、第１のコンテンツを出力させる際に、必ず第２のコンテンツを参照するようになり、第

1のコンテンツだけが出力されるようなことを防止できる。

第25の発明は、第23の発明の情報処理方法において、

上記第1の所定データは、第1のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第2のコンテンツの参照開始位置情報、参照終了位置情報を有するものである。このようにしたことによって、第1のコンテンツの第2のコンテンツへの挿入が、決められた位置に行われるようになる。

第26の発明は、第23の発明の情報処理方法において、

第2のコンテンツと上記秘密鍵に対応する公開鍵とを受信したとき、受信された上記第2のコンテンツと上記公開鍵を記録するようにしたものである。このようにしたことによって、その第2のコンテンツを利用する第1のコンテンツを受信したときに、記録された公開鍵と第2のコンテンツのデータを利用した処理が確実に実行できるようになる。

第27の発明は、第26の発明の情報処理方法において、

上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成し、

上記第1の所定データを所定のアルゴリズムに基づいて第2の所定データに変換し、

上記復号化データと上記第2の所定データとを照合するようにしたものである。このようにしたことによって、照合で一致した場合にだけ、記憶した第2のコンテンツを利用できるようになる。

第28の発明は、第27の発明の情報処理方法において、

上記照合の結果が一致した場合、上記第1の所定データに基づき、既に記録された第2のコンテンツを所定のタイミングで参照するようにしたものである。このようにしたことによって、第2のコンテンツを参照することが、確実に行えるようになる。

図面の簡単な説明

図１は、本発明の一実施の形態による放送システムの全体構成の例を示す構成図である。

図２は、本発明の一実施の形態によるシステムに適用される放送局の構成例を示すブロック図である。

図３は、本発明の一実施の形態によるシステムに適用される受信機の構成例を示すブロック図である。

図４は、図３に示した受信機をデータ処理上から見た構成で示したブロック図である。

図５は、本発明の一実施の形態による放送動作と受信動作を時間の流れで示した図である。

図６は、図５に示した処理を、データの流れで示した説明図である。

図７は、秘密鍵と公開鍵を使用した処理例を示した説明図である。

図８は、本発明の一実施の形態により過去のコンテンツを利用する例（番組紹介を行う例）を示した説明図である。

図９は、図８の例による処理を示したフローチャートである。

図１０は、本発明の一実施の形態により過去のコンテンツを利用する例（ＣＭを差し替える例）を示した説明図である。

図１１は、図１０の例による処理を示したフローチャートである。

図１２は、本発明の他の実施の形態による放送システムの全体構成の例を示す構成図である。

図１３は、図１２の例のシステムに適用される放送局の構成例を示すブロック図である。

図１４は、図１２の例のシステムに適用される鍵サーバの構成例を示すブロック図である。

図１５は、本発明の他の実施の形態による放送動作と受信動作を時間の流れで示した図である。

図１６は、図１２に示した処理を、データの流れで示した説明図である。

発明を実施するための最良の形態

以下、本発明の一実施の形態を、図１～図１１を参照して説明する。

図１は本例の放送システムの全体構成例を示した図である。本例においては、衛星放送によるテレビジョン放送システムに適用した例としてあり、ここでは第１の放送局１と第２の放送局２とが用意されて、両放送局１，２は何らかのネットワーク３で接続されている。このネットワーク３については、どのような通信手段であっても良く、電話回線，専用通信回線などが適用可能である。或いは、ネットワーク３として、インターネットや電子メールによるデータ伝送を利用しても良い。

第１の放送局１と第２の放送局２は、人工衛星４に対して所定のアップリンクで放送データを無線送信し、人工衛星４からのダウンリンクで各ユーザ側に設置された受信機１０に対して放送データを無線送信し、放送局１，２からの各種コンテンツ（番組）を、例えば各放送局毎に割当てられたチャンネルを使用して送信する。ここでは、受信機１０に接続された受像機５で、受信した放送の視聴を行う構成としてある。本例の受信機１０は、ハードディスクによる番組記録再生機能を内蔵させてある。なお、受信機１０と受像機５は一体化されている場合もある。

図２は、本例の放送局１，２の構成例を示す図である。本例では、映像コンテンツデータベース１０１と、オーディオコンテンツデータベース１０２と、公開鍵データベース１０３と、秘密鍵

データベース１０４と、データコンテンツデータベース１１１と、参照許可条件データベース１１４とが、データベースとして用意されている。公開鍵データベース１０３と、秘密鍵データベース１０４には、鍵発行サーバ１０５で生成された公開鍵及び秘密鍵をそれぞれ保存する。

映像コンテンツデータベース１０１とオーディオコンテンツデータベース１０２には、放送素材となる映像／オーディオ／データコンテンツを格納してある。映像コンテンツデータベース１０１から出力された映像コンテンツデータを、ビデオエンコーダ１０６でＭＰＥＧビデオストリームパケットにエンコードし、多重化装置１０８に供給する。オーディオコンテンツデータベース１０２から出力されたオーディオストリームパケットを、オーディオエンコーダ１０７でＭＰＥＧオーディオストリームパケットにエンコードし、多重化装置１０８に供給する。

多重化装置１０８では、映像パケットとオーディオパケットとに、データエンコーダ１０９から供給されるデータを多重化して、送出装置１１０に供給し、その多重化されたデータを放送データとして送出する。

データエンコーダ１０９では、データコンテンツデータベース１１１から供給されるデータコンテンツと公開鍵データベース１０３から供給される公開鍵のデータとを、ＭＰＥＧデータパケットに変換するエンコード処理を行い、処理されたＭＰＥＧデータパケットを、多重化装置１０８に供給する。

参照許可条件データベース１１４には、放送局に用意された各コンテンツに対して、その参照を許可する条件が登録してある。参照を許可する条件としては、例えば、放送局、コンテンツ中で参照を許可／禁止する部分、許可／禁止する提示方法、利用料金などがある。

この参照許可条件データベース１１４に格納されたデータと、秘密鍵データベース１０４に保持された秘密鍵のデータは、署名処理サーバ１１３に供給する。署名処理サーバ１１３は、署名を依頼される側の放送局であるとき（後述する図５の例の放送局１）、ネットワーク３を経由して受信したメタデータに署名を行い、メタデータの送信元に送信する。署名を依頼する側（後述する図５の例の放送局２）から提示されたメタデータには、参照先コンテンツ、参照位置、提示方法が記述されており、その内容が、事前に設定して参照許可条件データベース１１４に格納された参照許可条件と一致したとき、秘密鍵データベース１０４に保持された秘密鍵を使用して、メタデータに署名を行って、ネットワーク３を介して依頼元に送信する。

署名依頼処理サーバ１１２は、署名を依頼する側の放送局であるとき（後述する図５の例の放送局２）、署名を依頼される側の放送局に対して、メタデータをネットワーク３に送信し、署名されたメタデータをネットワーク３を介して受信して、その署名されたメタデータを、データコンテンツデータベース１１１に格納させる。

図３は、本例の受信機１０の構成例を示す図である。受信機１０は、セットトップボックス又はＩＲＤ（Integrated Receiver Decoder）と称される構成ものである。衛星４からの放送波を受信するアンテナ１１は、受信機１０内のチューナ部１２に接続してあり、チューナ部１２でこの受信機１０の中央制御ユニット（ＣＰＵ）２１から指示された所定のチャンネルを受信する。チューナ部１２で受信された信号（ベースバンド信号又は中間周波信号）は、復調部１３に供給して、伝送信号の変調方式に対応した復調処理を行う。具体的には、例えば８相ＰＳＫ復調，ＱＰＳＫ復調，６４ＱＡＭ復調などの伝送信号に対応した復調方式での復

調が行われる。

復調部１３で復調された受信信号は、ストリームデコーダ１４に供給して、トランスポートストリームと称されるデジタルデータを抽出する。このとき、受信データに多重化されている各種データを分離する処理し、例えば番組を構成するコンテンツの映像データと音声データを分離し、さらにそのコンテンツに付加されて伝送された各種データについても分離する。このコンテンツに付加されて伝送されたデータの１つとして、メタデータと称されるものがある。このメタデータには、コンテンツを構成する番組の映像データの表示形態や、音声データの出力形態などを規定するデータが含まれる。また、後述する鍵データがメタデータに含まれる場合もある。

ストリームデコーダ１４で抽出された映像データ及び音声データは、ここではＭＰＥＧ（Moving Picture Expers Group ）２方式で圧縮符号化されたデジタルデータであり、このＭＰＥＧ２方式の映像データ及び音声データのデコードを行うＭＰＥＧデコーダ１５に供給して、ＭＰＥＧ２方式からのデコードを行う。デコードされた映像データは、合成部１６で合成画像生成部１７から供給される映像データの合成処理を必要により行った後、映像出力部１９に供給し、接続された受像機（図示せず）の映像処理回路に供給する。合成画像生成部１７で生成させる合成用のデータについては、オンスクリーンディスプレイ（ＯＳＤ）と称される文字，数字，記号などをメインの画像に重畳して表示させるためのデータの他に、子画面表示やマルチ画像表示などを行うためのデータなどの各種形態の表示が行えるようなデータを生成できるようにしてある。後述するメタデータに基づいて蓄積されたコンテンツの映像データと受信したコンテンツの映像データとを合成するためのデータについても、この合成画像生成部１７で生成さ

れる。

また、ＭＰＥＧデコーダ１５でデコードされた音声データは、音声出力部１８から受像機（又はステレオ再生装置などの音声処理装置）の音声処理回路に供給する。

なお、受信機１０に接続された受像機などがデジタルデータを入力できる機器の場合には、映像出力部１９や音声出力部１８の出力は、デジタルデータのまま供給し、アナログ入力だけの機器が接続されている場合には、映像出力部１９や音声出力部１８でアナログ変換が必要である。また、受像機は受信機１０に一体化されている場合もある。

ここまでの放送信号を受信して出力するまでのそれぞれの処理は、この受信機１０が備える中央制御ユニット（ＣＰＵ）２１の制御で実行される。ＣＰＵ２１と受信機１０内の各回路とは内部バスで接続されている。また、この内部バスを介して制御用のプログラムなどが予め格納されたＲＯＭ２２と、ワークＲＡＭであるＲＡＭ２３とが接続してある。

さらに本例の受信機１０は、受信したコンテンツなどを記録するための大容量記憶手段としてのハードディスクドライブ（ＨＤＤ）２５を備え、そのＨＤＤ２５でのデータの記録及び再生を、内部バスに接続されたディスクコントローラ２４の制御で実行するようにしてある。例えば、受信してストリームデコーダ１４で抽出された所定のコンテンツの映像データ，音声データと、そのコンテンツのメタデータを、ディスクコントローラ２４の制御でＨＤＤ２５の所定のエリアに記録させる処理が行われる。そして、記録されたデータは、ディスクコントローラ２４の制御で読出されて、映像データや音声データについてはＭＰＥＧデコーダ１５に供給して、デコードされた後、接続された受像機などに再生データとして供給させる。読出されたメタデータについては、Ｃ

ＰＵ２１に供給し、映像データや音声データを処理する上で必要な制御処理を判断する。ＨＤＤ２５は、例えば数十Ｇバイト～数百Ｇバイトの記憶容量を有して、数十時間から数百時間分の映像データなどを記憶できる。

なお、ＨＤＤ２５の代わりに、例えば着脱自在な記録メディアを使用した記録手段を使用しても良い。

そして本例においては、ＨＤＤ２５に記憶させるコンテンツのメタデータに鍵データが付加されている場合には、該当するコンテンツがＨＤＤ２５に記録（蓄積）され続ける限りは、その鍵データについてもそのままＨＤＤ２５に記録させて保持させるようにしてある。ＨＤＤ２５に記録されたコンテンツのデータの読出しに、特に制限がない場合には、受信機１０の操作手段（図示せず）のユーザの操作に基づいて、任意のときに再生処理が行われる。

また、ＨＤＤ２５に記録されたコンテンツ（以下コンテンツＡとする）とは別のコンテンツ（以下コンテンツＢとする）を受信機１０が受信し、その受信したコンテンツＢに含まれるメタデータで、ＨＤＤ２５に記録されたコンテンツＡを参照することが指示されたときには、受信したコンテンツＢに含まれるメタデータ中の所定のデータを、ＨＤＤ２５に記録されたコンテンツＡのメタデータに含まれる鍵データで照合し、照合を確認したときだけ、コンテンツＡを参照した処理が行えるようにしてある。

なお、このとき照合に使用する鍵データは、コンテンツＡに対して放送局側で生成された秘密鍵（シークレットキー）データ及び公開鍵（パブリックキー）データの内の、公開鍵データであり、秘密鍵データについては公開されずに放送局内で保持される。この公開鍵と秘密鍵を使用した処理の詳細については後述する。

次に、このコンテンツＢがコンテンツＡを参照するデータ処理

から見た受信機１０の構成を図４に示す。受信機１０内のチューナ部１２で受信して復調部１３及びデコーダ１４で処理されたコンテンツのデータは、ＨＤＤ２５に蓄積させる場合には、ＨＤＤ２５内のコンテンツ格納部２５ａに格納され、そのコンテンツのメタデータ及び公開鍵データについては、ＨＤＤ２５内のメタデータ格納部２５ｂに格納される。ＨＤＤ２５内のコンテンツ格納部２５ａとメタデータ格納部２５ｂは、ディスクコントローラ２４の制御で仮想的に記録エリアが分割されて設定されるものである。

そして、この受信機１０でコンテンツＢを受信し、そのコンテンツＢのメタデータをＣＰＵ２１内の制御部２１ａが判断して、蓄積されたコンテンツＡを参照することが要求されている場合に、コンテンツＢのメタデータの内の一部のデータを、制御部２１ａからＣＰＵ２１内に構成される署名照合部２１ｂに送る。そして、この署名照合部２１ｂでは、そのデータの電子署名の照合を、ＨＤＤ２５に蓄積されたコンテンツＡのメタデータに付加された公開鍵データを使用して行い、照合が確認されたとき、ＨＤＤ２５に蓄積されたコンテンツＡを読出して、ＭＰＥＧデコーダ１５でのデコードを行い、コンテンツＢのデータのデコードについても行う。そして、デコードされたコンテンツＡ，Ｂの映像データ及び音声データを、コンテンツＢのメタデータで指示された態様で、合成部１６及び合成画像生成部１７を使用して合成処理（又は選択処理）して、この受信機１０から出力させる。

署名照合部２１ｂで電子署名の照合が確認できない場合には、ＭＰＥＧデコーダ１５でコンテンツＡのデコードを許可させず、コンテンツＢによる画像や音声の出力時にコンテンツＡを参照できないように制限させる。

次に、このようなコンテンツＢによるコンテンツＡの参照処理

の流れを、図５のチャートを参照して説明する。図５は、放送システム全体から見た流れの図であり、ここではコンテンツＡを図１に示した放送局１が送出し、コンテンツＢを図１に示した放送局２が送出し、それぞれのコンテンツＡ，Ｂを受信機１０で受信するものとする。

まず放送局１では、コンテンツＡを送出するに先立って、このコンテンツＡに対する秘密鍵データと公開鍵データの組を生成させ（ステップＳＴ１１）、コンテンツＡを放送する際に、そのとき生成された公開鍵データをメタデータに付加させる（ステップＳＴ１２）。受信機１０では、このコンテンツＡを受信して、このコンテンツＡを受信機１０内のＨＤＤ２５に蓄積させるとき、メタデータに付加された公開鍵データについても蓄積させる（ステップＳＴ１３）。

その後、放送局２でコンテンツＡを参照するコンテンツＢを生成させたとき、放送局２は、ネットワーク３経由で放送局１に対して、コンテンツＢのメタデータを送り、電子署名を依頼する（ステップＳＴ１４）。このとき放送局１では、放送局２からの依頼を許諾するか否か、依頼の条件や内容などから判断する。この依頼に応じるか否かは、例えばライセンス条件やコンテンツＡの利用料金などを判断して決める。

そして、依頼に応じるとき、コンテンツＢのメタデータの一部、又はコンテンツＢのメタデータに関連するデータに、コンテンツＡに対して生成させた秘密鍵データを使用して電子署名する（ステップＳＴ１５）。そして、その電子署名されたメタデータを放送局１から、ネットワーク３経由で放送局２に伝送する（ステップＳＴ１６）。

この電子署名されたメタデータを放送局２が受信した後には、その受信した電子署名されたメタデータをコンテンツＢに付加し

て（厳密にはコンテンツＢのデータ＋コンテンツＢの原メタデータ＋電子署名データ）、放送開始時間になるとコンテンツＢの送信を行う（ステップＳＴ１７）。

そして、この放送されたコンテンツＢを受信機１０が受信し、このコンテンツＢのメタデータでコンテンツＡを参照することが指示されていることを受信機１０内のＣＰＵ２１が判断すると、上記電子署名されたメタデータを、受信機１０内に蓄積されたコンテンツＡの公開鍵データを使用して復号化して復号化データを生成する。一方、コンテンツＢのメタデータも送信側が電子署名で使用した同じ所定のアルゴリズムでデータ変換を行い、変換データを生成する。そして、上記復号化データと上記変換データとの照合処理を行う。そして、この照合に成功したか否か判断し、照合に成功した場合だけ、コンテンツＢのメタデータで指示された方法で、蓄積されたコンテンツＡと受信したコンテンツＢとを合成して、受信機１０から出力させ、接続された受像機５で視聴させる（ステップＳＴ１８）。なお、コンテンツＢを受信すると同時に、コンテンツＡとコンテンツＢを合成させたデータの出力を行うのではなく、コンテンツＢについても受信機１０内のＨＤＤ２５に蓄積させて、その蓄積されたコンテンツＢを出力させるとき、コンテンツＡを参照して合成などを行うようにしても良い。

図６は、図５のフローチャートで示した処理を、データの流れから見た図である。図６の中のステップ数は、図５に一致させてある。コンテンツＡを放送した放送局１では、秘密鍵データと公開鍵データとを生成させて、コンテンツＡを放送する際には、コンテンツＡのデータに公開鍵データが付加されている。コンテンツＡを参照するコンテンツＢを放送する放送局２では、放送局１との間で、メタデータの署名の依頼と、その依頼したメタデータ

の返送が行われる。そして放送局２は、この署名されたメタデータが付加されたコンテンツＢを放送する。

ここで、秘密鍵データと公開鍵データとを使用した電子署名の処理例について、図７を参照して説明する。まず、電子署名したいコンテンツＢのメタデータがある場合、そのメタデータのメッセージダイジェストを作成する（ステップＳＴ２１）。なお、このときのメタデータには、コンテンツＡの参照命令を少なくとも含むものである。また、ここでのメッセージダイジェストとは、元のデータの特徴を表す固定長（例えば１２８ビット程度）のビットパターンで、予め決められた所定のアルゴリズムで生成される。このメッセージダイジェストは、異なるデータに対して同じメッセージダイジェストが生成される確率は極めて低く、メッセージダイジエストが変わらないように元のデータ（メタデータ）を改変することは実質上不可能である。

このメッセージダイジェストの生成は、例えば放送局２側で行う（放送局１側で行っても良い）。そして、そのメッセージダイジェストを放送局１に送って、放送局１に保持された秘密鍵データを使用して暗号化して、電子署名されたデータとする（ステップＳＴ２２）。この際に使用される公開鍵暗号系としては、ＲＳＡ方式などが知られている。そして放送局２内では、この電子署名されたメッセージダイジェストのデータを、コンテンツＢのメタデータに付加して放送する（ステップＳＴ２３）。

そして、コンテンツＢを受信した受信機内では、そのコンテンツＢのメタデータに付加された電子署名されたメッセージダイジェストのデータを抽出し、そのデータを受信機内で保持されたコンテンツＡの公開鍵データで復号する（ステップＳＴ２４）。また受信機内で、コンテンツＢのメタデータから、メッセージダイジェストを生成させる（ステップＳＴ２５）。このときには、ス

テップＳＴ２１でメッセージダイジェストを生成させた際と同じアルゴリズムを使用して生成させる。そして、生成されたメッセージダイジェストと復号されたデータとを受信機内で比較し（ステップＳＴ２６）、一致したとき、受信機内で電子署名を確認したものと判断する。

次に、このような処理で実行されるコンテンツＢによるコンテンツＡの参照処理の例を説明する。図８は、コンテンツＢがコンテンツＡの番組紹介を行うコンテンツである例である。ステップＳＴ３１でコンテンツＡが、メタ（１）に記述された公開鍵と共に放送されて、そのデータが受信機で蓄積された後、ステップＳＴ３２でそのコンテンツＡを参照するコンテンツＢが送信されたとき、受信機に接続された受像機の画面では、メタ（２）の記述に従い、コンテンツＡの映像データＡＶ（１）の主要な場面の画像などが縮小されて表示され、コンテンツＢの映像データＡＶ（２）による番組の紹介者などの画像などが合成されて表示される。ここでメタ（２）には、参照されるＡＶ（１）および参照範囲（開始／終了位置）、ＡＶ（１）およびＡＶ（２）の画面上での表示位置／縮小比率／タイミングに関する情報が、これらの記述に対する電子署名と共に記述される。また、コンテンツＡの番組の内容をメタ（２）中にテキストデータとして記述しておき、その内容を文字などで紹介する画像についても、コンテンツＢのデータであるメタ（２）の指示（すなわち表示位置／タイミング、表示書式など）に基づいて受信機内で生成されて、同時に表示されるようにしても良い。また、音声についても、コンテンツＡの番組の音声の一部に、コンテンツＢによる音声を合成させても良い。

この図８に示した例でのメタデータの例を示すと、以下のようになる。

```
<メタデータ>
……
  <参照ｉｄ＝“Ｒ１”>
   <参照先>
    <コンテンツ>ＡＶ１</コンテンツ>
    <開始位置>ｔ１</開始位置>
    <終了位置>ｔ２</終了位置>
   </参照先>
   <提示形態>
    <子画面表示>
     <参照ｺﾝﾃﾝﾂ表示位置>(Ｘ A, Ｙ A)</参照ｺﾝﾃﾝﾂ表示位置>
     <参照ｺﾝﾃﾝﾂ縮小率>50％</参照ｺﾝﾃﾝﾂ縮小率>
     <ｵﾘｼﾞﾅﾙｺﾝﾃﾝﾂ表示位置>(Ｘ B, Ｙ B)</ｵﾘｼﾞﾅﾙｺﾝﾃﾝﾂ表示位置>
     <ｵﾘｼﾞﾅﾙｺﾝﾃﾝﾂ縮小率>50％</ｵﾘｼﾞﾅﾙｺﾝﾃﾝﾂ縮小率>
     <表示タイミング>ｔ３</表示タイミング>
    </子画面表示>
   </提示形態>
  </参照>
  ……
  <署名>
   <Signature xmlns="http://www.w3c.org/2000/09/xmldsig#">
    <SignedInfo>
     ……
      <ReferenceURI= “#R1” >....</Reference>
    </SignedInfo>
   <Signature>
  </署名>
</メタデータ>
```

この例のメタデータの署名部分は、ＸＭＬ－Signature の仕様に従った記述である。この例では、署名の対象が＜参照ｉｄ＝“Ｒ１”＞から始まる部分であることが示されている。また、子画面表示の表示形態として、１画面中での表示位置（X_A, Y_A）及び（X_B, Y_B）（図８参照）と、表示される縮小率が指定されて、図８に示したような子画面表示が行われる状態を指定している。

図９は、この図８の例による端末側での処理例を示したフローチャートである。このフローチャートに従って説明すると、まずステップＳ１１において、復調部１３及びストリームデコーダ１４にて、入力ストリームデータを、コンテンツとメタデータに分離する。

次にステップＳ１２において、制御部２１ａにてメタデータをパーズし、「参照」要素及び対応する「署名」要素の内容を抽出する。そしてステップＳ１３において、署名照合部２１ｂにて、「参照」要素中の「コンテンツ」要素の内容を元に、事前に蓄積しておいたコンテンツＡの公開鍵をメタデータ格納部２５ｂから取り出す。

そしてステップＳ１４において、署名照合部２１ｂにて、取り出した公開鍵を用いて、「参照」／「署名」の内容を照合する。

このとき、ステップＳ１５で、照合に成功したか否か判断し、照合に成功しないときには、ステップＳ１６に移り、処理を中断させる。また、照合に成功した場合には、ステップＳ１７に移り、デコーダ１５，合成部１６，合成画像生成部１７において、制御部２１ａと署名照合部２１ｂの指示に基づき、ストリームデコーダ１４から出力されるストリームである、コンテンツＢのデコード及び表示を開始させる。

その後、ステップＳ１８に移り、時刻ｔ₃まで待機する。さら

にステップＳ１９に移り、デコーダ１５において、署名照合部２１ｂの指示に基づき、メタデータ格納部２５ａに格納されているコンテンツＡについて、タイミングt_1からタイミングt_2までのデコードを開始する。このとき同時に、制御部２１ａの指示に基づき合成部１６及び合成画像生成部１７でのコンテンツＡ及びＢの合成及び表示を開始させる。

ここでは番組紹介を行う例としたが、他の参照処理を行うようにしても良い。例えば、コンテンツＡとしてサッカーゲームなどのスポーツ中継の番組とし、コンテンツＢとして、そのスポーツ中継のハイライトシーンなどの一部の場面だけを紹介するスポーツニュース番組としてのコンテンツとし、コンテンツＢを視聴させるとき、コンテンツＡとして蓄積された画像の中のハイライトシーンを順に紹介するような画像や音声を出力させても良い。

また、映画やドラマなどのコンテンツ（コンテンツＡ）を語学学習用の教材として参照するような場合に、コンテンツＢでその参照するようなデータを送り、図８に示したような番組紹介の代わりに、コンテンツＡの映像や音声に何らかの編集処理を施して、その映像や音声の出力と同時にセリフの原語表示，翻訳表示などを文字で行ったり、翻訳された音声を出力させるようにしても良い。

このように本例の処理を行うことで、既に送られて蓄積されたコンテンツＡを参照するコンテンツＢの視聴が可能になるが、いずれの場合でも、受信機側では公開鍵データを使用して一致が確認できた場合にだけ、このような参照処理を行うので、コンテンツＡを送出させた放送局側が秘密鍵データを外部に漏らさない限りは、コンテンツＡを送出させた放送局で承認がされない限り、コンテンツＡを参照する視聴が行えないので、著作権などを侵害するような形での他のコンテンツの参照を効果的に防止できる。

また、図１０は、コンテンツＢによるコンテンツＡの参照処理として、コンテンツＡの映像及び音声の一部を、コンテンツＢの映像及び音声に置き替える場合の例である。即ち、図１０Ａに示すように、コンテンツＡによる番組として、シーン１，シーン２，シーン３などの場面の変化時に、特定のコマーシャルＣＭ１，ＣＭ２，ＣＭ３‥‥を入れてあるものとする。このとき、コンテンツＢとして、図１０Ｂに示すように、このコンテンツＡのコマーシャルＣＭ１，ＣＭ２，ＣＭ３‥‥を置き替えるコマーシャルＣＭ１１，ＣＭ１２，ＣＭ１３‥‥の映像及び音声を送る。この場合には、コンテンツＢのデータについても、受信機内のＨＤＤに蓄積させる。このデータにはコンテンツＡにおけるＣＭ１，ＣＭ２，ＣＭ３‥‥の開始／終了位置、コンテンツＢにおけるＣＭ１１，ＣＭ１２，ＣＭ１３‥‥の開始／終了位置、およびＣＭ１とＣＭ１１、ＣＭ２とＣＭ１２、‥‥を置き替えることを指示するコマンドが、これらの記述に対する電子署名と共に記述される。そして、コンテンツＢを受信した後にコンテンツＡの番組を視聴するときには、図１０Ｃに示すように、ＨＤＤ中に格納されたデータの指示に従って、コマーシャルＣＭ１，ＣＭ２，ＣＭ３‥‥をコマーシャルＣＭ１１，ＣＭ１２，ＣＭ１３‥‥に置き替えて出力させて視聴させる。

この図１０に示した例でのメタデータの例を示すと、以下のようになる。

<メタデータ>

……

<参照ｉｄ＝“R1”>

<参照先>

<コンテンツ>コンテンツＡ</コンテンツ>

<開始位置>s_1</開始位置>

<終了位置>e 1</終了位置>
</参照先>
<提示形態>
<置換>
<コンテンツ>コンテンツA</コンテンツ>
<開始位置>s 11</開始位置>
<終了位置>e 11</終了位置>
</置換>
</提示形態>
</参照>
<参照 i d = "R2" > ....</参照> (→CM2,CM12に関する記述)
<参照 i d = "R3" > ....</参照> (→CM3,CM13に関する記述)
……
<署名>
<Signature xmlns="http://www.w3c.org/2000/09/xmldsig#">
<SignedInfo>
……
<ReferenceURI= "#R1" >....</Reference>
</SignedInfo>
<Signature>
</署名>
<署名>.....</署名> (→ <参照id= "R2" > 部分の署名)
<署名>.....</署名> (→ <参照id= "R3" > 部分の署名)
</メタデータ>

このメタデータの例の内の括弧書きの部分は、メタデータの内容を説明したものである。この例のメタデータの署名部分についても、ＸＭＬ－Signature の仕様に従った記述であり、<ReferenceURI= "#R1" > との記述は、署名の対象が <参照 i d = "R1

”＞から始まる部分であることを表している。

この例では、＜参照先＞として、コンテンツＡのＣＭ１の開始位置s_1と終了位置e_1が記述されている。また、提示形態が＜置換＞であるコンテンツＢのＣＭ１１の開始位置s_{11}と終了位置e_{11}が記述され、コンテンツＡのＣＭ１が、コンテンツＢのＣＭ１１に置換されることを表している。

図１１は、この図１０の例による端末側での処理例を示したフローチャートである。このフローチャートに従って説明すると、まずステップＳ２１において、復調部１３及びストリームデコーダ１４にて、入力ストリームデータを、コンテンツとメタデータに分離し、ストリームデータをコンテンツ格納部２５ａに格納させ、メタデータをメタデータ格納部格納部２５ｂに格納させる。

次に、ステップＳ２２において、制御部２１ａにて、メタデータをパーズし、各「参照」要素および対応する「署名」要素の内容を抽出する。そしてステップＳ２３で、署名照合部２１ｂにて、「参照」要素中の「コンテンツ」要素の内容を元に、事前に蓄積しておいたコンテンツＡの公開鍵をメタデータ格納部２５ｂから取り出す。

この公開鍵が取り出されると、ステップＳ２４に移って、署名照合部２１ｂにて、取り出した公開鍵を用いて、各「参照」／「署名」の内容を照合する。そして、ステップＳ２５で、この照合に成功したか否か判断する。照合に失敗したときには、ステップＳ２６に移って、処理を中断する。

照合に成功した場合には、ステップＳ２７に移り、デコーダ１５，合成部１６，合成画像生成部１７において、制御部２１ａと署名照合部２１ｂの指示に基づき、コンテンツ格納部２５ａに格納されたコンテンツＡのデコード及び表示を開始させる。

その後、ステップＳ２８に移り、全ての処理が完了したか否か

判断し、全ての処理が終了したと判断したとき、ステップＳ２９に移り、コンテンツＡの残りを再生して終了する。

ステップＳ２８で、全ての処理が完了してないと判断したとき、ステップＳ３０に移る。ここで、残りの参照のうち開始位置が最も早いものの開始位置をs_i、終了位置をe_iとするとき（図１０Ａ参照）、コンテンツＡの再生が開始位置s_iに差し掛かるまで待つ。

そしてステップＳ３１に移り、デコーダ１５，合成部１６，合成画像生成部１７において、制御部２１ａと署名照合部２１ｂの指示に基づき、コンテンツＡの再生を中断し、替わりに「置換」要素の内容に従って、コンテンツＢのＣＭ１１部分のデコードとそのデコードされたデータの表示を、開始位置s_n（図１０Ｂ参照）から行われる。

その後、さらにステップＳ３２に移り、デコーダ１５，合成部１６，合成画像生成部１７において、制御部２１ａと署名照合部２１ｂの指示に基づき、終了位置e_n（図１０Ｂ参照）でコンテンツＢの再生を終了し、位置e_iからコンテンツＡの再生を再開させる。

この図１０，図１１に示すように処理することで、例えば最初にコンテンツＡに含まれたコマーシャルで宣伝する内容に時期的な有効期限などがある場合、その期限が切れた時点で、新たなコマーシャルをコンテンツＢとして送ることで、ユーザ側では常に最新のコマーシャルを視聴できるようになる。この場合、最初にコンテンツＡに入っていたコマーシャルと差し替えることが承認されない限り、別のコマーシャルに差し替えられることはないので、そのコマーシャルを流しているスポンサーの権利を侵害するような形で差し替えられることはない。

なお、ここまでの説明では、各コンテンツの鍵データは、放送

局が保持するようにしたが、放送局とは別の鍵管理サーバ（鍵管理会社）をネットワーク上に設けて、その鍵管理サーバが秘密鍵データや公開鍵データを管理するようにしても良い。図１２はその場合のシステム構成例を示した図であり、放送局１，２に接続されたネットワーク３には、鍵管理サーバ６が接続されている。

図１３は、放送局１，２と鍵管理サーバ６とを別にした場合の、放送局１，２の構成例を示した図である。

この例では、映像コンテンツデータベース１０１と、オーディオコンテンツデータベース１０２と、公開鍵データベース１０３と、データコンテンツデータベース１１１とが、データベースとして用意されている。公開鍵データベース１０３には、公開鍵を保存する。

映像コンテンツデータベース１０１とオーディオコンテンツデータベース１０２には、放送素材となる映像／オーディオ／データコンテンツを格納してある。映像コンテンツデータベース１０１から出力された映像コンテンツデータを、ビデオエンコーダ１０６でＭＰＥＧビデオストリームパケットにエンコードし、多重化装置１０８に供給する。オーディオコンテンツデータベース１０２から出力されたオーディオストリームパケットを、オーディオエンコーダ１０７でＭＰＥＧオーディオストリームパケットにエンコードし、多重化装置１０８に供給する。

多重化装置１０８では、映像パケットとオーディオパケットとに、データエンコーダ１０９から供給されるデータを多重化して、送出装置１１０に供給し、その多重化されたデータを放送データとして送出する。

データエンコーダ１０９では、データコンテンツデータベース１１１から供給されるデータコンテンツと公開鍵データベース１０３から供給される公開鍵のデータとを、ＭＰＥＧデータパケッ

トに変換するエンコード処理を行い、処理されたＭＰＥＧデータパケットを、多重化装置１０８に供給する。

署名依頼処理サーバ１１２は、署名を依頼する側の放送局であるとき、署名を依頼される側に対して、メタデータをネットワーク３に送信し、署名されたメタデータをネットワーク３を介して受信して、その署名されたメタデータを、データコンテンツデータベース１１１に格納させる。

図１４は、鍵管理サーバ６の構成例を示した図である。鍵管理サーバ６は、データベースとして、公開鍵データベース２０１と、秘密鍵データベース２０２と、参照許可条件データベース２０３とを備える。公開鍵データベース２０１と、秘密鍵データベース２０２が格納する公開鍵及び秘密鍵は、鍵発行サーバ２０４が生成させたものである。署名処理サーバ２０５は、ネットワーク３を介してメタデータに署名依頼があるとき、参照許可条件データベース２０３に格納された参照条件を満たすとき、秘密鍵データベース２０２が格納した秘密鍵を使用して、メタデータに署名して、依頼した放送局側にネットワーク３を介して送信する。

図１５は、この鍵管理サーバ６を使用した場合のコンテンツＡ，Ｂの送出処理例を示した図である。まず、コンテンツＡを送出する放送局１では、そのコンテンツＡを他のコンテンツが利用する際のライセンス条件を、鍵管理サーバ６に登録させる（ステップＳＴ４１）。そして、鍵管理サーバ６では、コンテンツＡに対する秘密鍵データと公開鍵データを生成させ（ステップＳＴ４２）、公開鍵データだけを放送局１に送る（ステップＳＴ４３）。秘密鍵データについては、鍵管理サーバ６内で保持させておく。

ここまでの処理が行われた後に、放送局１はコンテンツＡに公開鍵データをメタデータを付加して送信する（ステップＳＴ４４）。受信機１０では、このコンテンツＡを受信して、このコンテ

ンツＡを受信機１０内のＨＤＤ２５に蓄積させるとき、メタデータに付加された公開鍵データについても蓄積させる（ステップＳＴ４５）。

その後、放送局２でコンテンツＡを参照するコンテンツＢを生成させたとき、放送局２は、ネットワーク３経由で鍵管理サーバ６に対して、コンテンツＢのメタデータを送り、電子署名を依頼する（ステップＳＴ４６）。このとき鍵管理サーバ６では、コンテンツＡに対して登録されたライセンス条件のデータを、放送局２に送り（ステップＳＴ４７）、そのライセンス条件に同意するデータが鍵管理サーバ６に送られたとき（ステップＳＴ４８）、コンテンツＢのメタデータから生成されたメッセージダイジェストに、コンテンツＡに対して生成させた秘密鍵データを使用して電子署名する（ステップＳＴ４９）。そして、その電子署名されたメタデータを鍵管理サーバ６から、ネットワーク３経由で放送局２に伝送する（ステップＳＴ５０）。

この電子署名されたメタデータを放送局２が受信した後には、その受信した電子署名されたデータをコンテンツＢのメタデータに付加して、放送開始時間になるとコンテンツＢの送信を行う（ステップＳＴ５１）。

そして、この放送されたコンテンツＢを受信機１０が受信し、このコンテンツＢのメタデータでコンテンツＡを参照することが指示されていることを受信機１０内のＣＰＵ２１が判断すると、コンテンツＢのメタデータの一部を、受信機１０内に蓄積されたコンテンツＡの公開鍵データを使用して照合し、照合に成功したか否か判断し、照合に成功した場合だけ、コンテンツＢのメタデータで指示された方法で、蓄積されたコンテンツＡと受信したコンテンツＢとを合成して、受信機１０から出力させ、接続された受像機５で視聴させる（ステップＳＴ５２）。

図１６は、図１５のフローチャートで示した処理を、データの流れから見た図である。図１６の中のステップ数は、図１５に一致させてある。コンテンツＡを放送した放送局１とは別の鍵管理サーバ６では、秘密鍵データと公開鍵データとを生成させて保持させてある。そして、放送局１がコンテンツＡを放送する際には、コンテンツＡのデータに公開鍵データが付加されている。コンテンツＡを参照するコンテンツＢを放送する放送局２では、鍵管理サーバ６との間で、メタデータの署名の依頼と、その依頼したメタデータの返送が行われる。そして放送局２は、この署名されたメタデータが付加されたコンテンツＢを放送する。

このように放送局とは別の鍵管理サーバを設けたことでも、上述した図１～図１１に示した処理と同様の処理が可能になる。

なお、上述した実施の形態では、コンテンツＡを配信する第１の放送局１とコンテンツＢを配信する第２の放送局２とが別の放送局である例としたが、コンテンツＡ，Ｂを配信する放送局が同じであっても良い。なお、ここでの放送局とは、コンテンツを送信させるいわゆる送信所として示したが、放送局ではコンテンツの配信や管理だけを行って、そのコンテンツの送信については、別の送信所から行う構成であっても良い。

また、上述した実施の形態では、衛星放送を利用した放送システムに適用した例としたが、他の伝送路による放送システムにも適用可能である。この場合、予め規定された伝送チャンネルで放送を行うテレビジョン放送やラジオ放送のような一般的な意味での放送だけでなく、無線又は有線の伝送路を使用して不特定多数のユーザにコンテンツを配信するサービスであれば適用可能であり、例えばいわゆるインターネット放送のような、何らかのネットワークで接続された不特定多数のユーザ（或いは予め契約された複数のユーザ）の端末（受信機）に対して、サーバ（放送局）

側から各種コンテンツを配信させる際にも、本発明を適用することが可能である。

また、上述した実施の形態の説明では、後から送信されるコンテンツが参照する過去のコンテンツは、１つのコンテンツだけとしたが、蓄積された複数のコンテンツを参照するような場合にも適用可能である。

また、上述した実施の形態では、放送される各コンテンツのスクランブル処理については何も説明しなかったが、何らかのスクランブル処理を施して放送して、契約された特定のユーザの受信機だけが受信できるようにしても良い。この場合、元のコンテンツＡを参照するコンテンツＢを視聴する際にだけ、スクランブルがかかるようにして、契約（課金）されたユーザだけがコンテンツＢによる視聴ができるようにしても良い。逆に、コンテンツＡに対してスクランブルを施し、コンテンツＢによる参照時（例えば番組紹介など）にはスクランブルがかからないようにして、課金処理を行ったユーザだけが、コンテンツＡを完全に視聴できるようにしても良い。

また、上述した実施の形態では、放送信号として放送局から受信端末に伝送する場合について説明したが、放送以外の形態でストリームデータを伝送する場合にも適用可能である。

また、上述した実施の形態では、放送局及び受信機のいずれも、データ格納手段やエンコーダ，デコーダなどを専用の回路で構成させるようにしたが、例えば同様の処理を実行するソフトウェアを、コンピュータ装置などのデータ処理装置に組み込んで、放送局又は受信機として機能するようにしても良い。この場合、ソフトウェアは、ディスク，テープ，メモリカードなどの媒体に記憶させて配付する他に、インターネットなどの伝送媒体を使用して配付するようにしても良い。

産業上の利用可能性

本発明にかかる情報処理方法、情報処理装置、電子機器及び媒体によると、最初に送ったコンテンツの管理者に参照することが許可された場合にだけ、正しい署名が行われた所定データが別のコンテンツに付加されるので、最初に送信されたコンテンツを蓄積した各受信者側の設備では、そのコンテンツを参照しても良いと許可されたコンテンツを受信したときだけ、自動的に別のコンテンツが参照するようになる。従って、過去のコンテンツの製作者や放送業者の権利を守った上で、随時その過去のコンテンツを参照した新たなコンテンツを制作して配信できるようになる。

この場合、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部を利用した別のコンテンツを作成して視聴させることが良好にできるようになる。

また、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツの一部の画像や音声などを最新のデータに置き替えて視聴させることができるようになる。

さらに、過去のコンテンツの管理者に許可された場合にだけ、例えば過去の特定のコンテンツのハイライトシーンだけを表示させるようなことが可能になる。

請 求 の 範 囲

1．ネットワークを介して情報の授受を行う情報処理装置において、

上記第１のコンテンツに対して、秘密鍵と公開鍵を生成させて管理する鍵管理手段と、

上記鍵管理手段で管理する公開鍵を付加して、上記第１のコンテンツを送信する第１の送信手段と、

上記第２のコンテンツに付加される所定データに対して、上記鍵管理手段が管理する秘密鍵での電子署名を要求し、その電子署名された所定データが付加された上記第２のコンテンツを送信する第２の送信手段とを備えたこと

を特徴とする情報処理装置。

2．上記鍵管理手段は、上記第２の送信手段からの電子署名要求時に、上記第２のコンテンツによる第１のコンテンツの参照が、第１のコンテンツの所定の権利を侵害しないと判断したときだけ、上記所定データへの電子署名を実行すること

を特徴とする請求項１記載の情報処理装置。

3．ネットワークを介して情報の授受を行う情報処理装置において、

第１のコンテンツと、第１のコンテンツに関連する所定データとを、第２のコンテンツに適用される秘密鍵を用いて上記所定データに電子署名を行った電子署名データに組み合わせて送信する第１の送信手段を備えること

を特徴とする情報処理装置。

4．上記電子署名データを取得する電子署名データ取得手段を有すること

を特徴とする請求項３記載の情報処理装置。

5．上記秘密鍵を使用して電子署名が行われる上記所定データは

、上記第２のコンテンツの参照命令を含むこと
を特徴とする請求項３記載の情報処理装置。

６．上記所定データは、第１のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有すること
を特徴とする請求項５記載の情報処理装置。

７．コンテンツデータを受信する受信手段と、
上記受信手段が受信したコンテンツを蓄積するコンテンツ蓄積手段と、
上記コンテンツ蓄積手段に蓄積された第１のコンテンツに付加された鍵データを使用して、上記受信手段が受信した第２のコンテンツに付加された所定データの電子署名を照合する照合手段と、
上記照合手段での照合が成功したとき、上記コンテンツ蓄積手段に蓄積された第１のコンテンツを、上記第２のコンテンツでの指示に基づいて加工するコンテンツ加工手段と、
上記コンテンツ加工手段で加工されたコンテンツを出力するコンテンツ出力手段とを備えた
電子機器。

８．上記コンテンツ加工手段での加工は、上記第１のコンテンツによる画像又は音声と上記第２のコンテンツによる画像又は音声を合成する処理であること
を特徴とする請求項７記載の電子機器。

９．上記コンテンツ加工手段での加工は、上記第１のコンテンツによる画像又は音声の一部を、上記第２のコンテンツによる画像又は音声に置き替える処理であること
を特徴とする請求項７記載の電子機器。

10．上記コンテンツ加工手段での加工は、上記第１のコンテンツ

による画像又は音声を、第２のコンテンツによる指示で編集する処理であること

を特徴とする請求項７記載の電子機器。

11. ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する電子機器において、

第１のコンテンツと、上記第１のコンテンツに関連する第１の所定データと、第２のコンテンツに適用される秘密鍵を上記第１の所定データに用い生成された電子署名データとの組み合わせデータを受信する第１の受信手段を有すること

を特徴とする電子機器。

12. 上記秘密鍵を使用して電子署名が行われる上記第１の所定データは、第２のコンテンツの参照命令を含むこと

を特徴とする請求項１１記載の電子機器。

13. 上記第１の所定データは、第１のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有すること

を特徴とする請求項１２記載の電子機器。

14. 第２のコンテンツと上記秘密鍵に対応する公開鍵とを受信する第２の受信手段と、

受信された上記第２のコンテンツと上記公開鍵を記憶する記憶手段とを有すること

を特徴とする請求項１１記載の電子機器。

15. 上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成する復号化手段と、

上記第１の所定データを所定のアルゴリズムに基づいて第２の所定データに変換するデータ変換手段と、

上記復号化手段により生成された上記復号化データと、上記データ変換手段により変換された上記第２の所定データとを照

合する照合手段とを有すること

を特徴とする請求項１４記載の電子機器。

16. 上記照合手段の照合結果が一致した場合、上記第１の所定データに基づき上記記憶手段に記憶された第２のコンテンツを所定のタイミングで参照する参照手段とを有すること

を特徴とする請求項１５記載の電子機器。

17. 第１のコンテンツと、この第１のコンテンツを参照する第２のコンテンツを処理する情報処理方法において、

上記第１のコンテンツに対して、秘密鍵と公開鍵を生成させ、

上記生成された公開鍵を付加して、上記第１のコンテンツを送信し、

上記第２のコンテンツに付加される所定データに対して、上記秘密鍵での電子署名を要求し、

上記電子署名された所定データが付加された上記第２のコンテンツを送信すること

を特徴とする情報処理方法。

18. 送信される上記第１のコンテンツを受信して蓄積した状態で、送信される上記第２のコンテンツを受信した場合に、蓄積された第１のコンテンツに付加された公開鍵を使用して、上記所定データの電子署名を照合し、

その照合に成功したとき、受信した上記第２のコンテンツの指示に基づいて、上記蓄積された第１のコンテンツに所定の加工を施して出力すること

を特徴とする請求項１７記載の情報処理方法。

19. ネットワークを介して情報の授受を行う情報処理方法において、

第１のコンテンツと、第１のコンテンツに関連する所定デー

タとを送信する場合に、

上記第１のコンテンツとは別の第２のコンテンツに適用される秘密鍵を用いて、上記所定データに電子署名を行い、

その電子署名された電子署名データを上記所定データに組み合わせて送信する

を特徴とする情報処理方法。

20. 上記秘密鍵を用いた電子署名を、上記第２のコンテンツ又は上記秘密鍵を管理する側に依頼し、その依頼に基づいて得られた電子署名データを、上記所定データに組み合わせること

を特徴とする請求項１９記載の情報処理方法。

21. 上記秘密鍵を使用して電子署名が行われる上記所定データは、上記第２のコンテンツの参照命令を含むこと

を特徴とする請求項１９記載の情報処理方法。

22. 上記所定データは、第１のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有すること

を特徴とする請求項２１記載の情報処理方法。

23. ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する情報処理方法において、

第１のコンテンツを記録するとき、上記第１のコンテンツに関連する第１の所定データと、既に記録された第２のコンテンツに適用される秘密鍵を上記第１の所定データに用い生成された電子署名データとを記録すること

を特徴とする情報処理方法。

24. 上記秘密鍵を使用して電子署名が行われる上記第１の所定データは、第２のコンテンツの参照命令を含むこと

を特徴とする請求項２３記載の情報処理方法。

25. 上記第１の所定データは、第１のコンテンツに対する挿入開

始位置情報、挿入終了位置情報及び対応する第２のコンテンツの参照開始位置情報、参照終了位置情報を有すること

を特徴とする請求項２４記載の情報処理方法。

26. 第２のコンテンツと上記秘密鍵に対応する公開鍵とを受信したとき、受信された上記第２のコンテンツと上記公開鍵を記録すること

を特徴とする請求項２３記載の情報処理方法。

27. 上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成し、

上記第１の所定データを所定のアルゴリズムに基づいて第２の所定データに変換し、

上記復号化データと上記第２の所定データとを照合すること

を特徴とする請求項２６記載の情報処理方法。

28. 上記照合の結果が一致した場合、上記第１の所定データに基づき、既に記録された第２のコンテンツを所定のタイミングで参照すること

を特徴とする請求項２７記載の情報処理方法。

29. 第１のコンテンツと、この第１のコンテンツを参照する第２のコンテンツを処理する情報処理を実行するプログラムを格納又は伝送する媒体において、

上記第１のコンテンツに対して、秘密鍵と公開鍵を生成させ、

上記生成された公開鍵を付加して、上記第１のコンテンツを送信し、

上記第２のコンテンツに付加される所定データに対して、上記秘密鍵での電子署名を要求し、

上記電子署名された所定データが付加された上記第２のコン

テンツを送信する処理を行う

ことを特徴とするプログラムを格納又は伝送する

媒体。

30. 上記プログラムは、さらに、

送信される上記第１のコンテンツを受信して蓄積した状態で、送信される上記第２のコンテンツを受信した場合に、蓄積された第１のコンテンツに付加された公開鍵を使用して、上記所定データの電子署名を照合し、

その照合に成功したとき、受信した上記第２のコンテンツの指示に基づいて、上記蓄積された第１のコンテンツに所定の加工を施して出力すること

を特徴とする請求項２９記載の媒体。

31. ネットワークを介して情報の授受を行う情報処理を実行するプログラムを格納又は伝送する媒体において、

第１のコンテンツと、第１のコンテンツに関連する所定データとを送信する場合に、

上記第１のコンテンツとは別の第２のコンテンツに適用される秘密鍵を用いて、上記所定データに電子署名を行い、

その電子署名された電子署名データを上記所定データに組み合わせて送信する

ことを特徴とするプログラムを格納又は伝送する

媒体。

32. 上記プログラムは、さらに、

上記秘密鍵を用いた電子署名を、上記第２のコンテンツ又は上記秘密鍵を管理する側に依頼し、その依頼に基づいて得られた電子署名データを、上記所定データに組み合わせること

を特徴とする請求項３１記載の媒体。

33. 上記プログラムは、さらに、

上記秘密鍵を使用して電子署名が行われる上記所定データには、上記第2のコンテンツの参照命令を含ませること
を特徴とする請求項31記載の媒体。

34. 上記プログラムは、さらに、
上記所定データは、第1のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第2のコンテンツの参照開始位置情報、参照終了位置情報を有すること
を特徴とする請求項33記載の媒体。

35. ネットワークを介して情報の授受を行い、それら情報を記録及び／又は再生する情報処理を実行するプログラムを格納又は伝送する媒体において、
第1のコンテンツを記録するとき、上記第1のコンテンツに関連する第1の所定データと、既に記録された第2のコンテンツに適用される秘密鍵を上記第1の所定データに用い生成された電子署名データとを記録する
ことを特徴とするプログラムを格納又は伝送する
媒体。

36. 上記プログラムは、さらに、
上記秘密鍵を使用して電子署名が行われる上記第1の所定データには、第2のコンテンツの参照命令を含ませること
を特徴とする請求項35記載の媒体。

37. 上記プログラムは、さらに、
上記第1の所定データに、第1のコンテンツに対する挿入開始位置情報、挿入終了位置情報及び対応する第2のコンテンツの参照開始位置情報、参照終了位置情報を含ませること
を特徴とする請求項36記載の媒体。

38. 上記プログラムは、さらに、
第2のコンテンツと上記秘密鍵に対応する公開鍵とを受信し

たとき、受信された上記第２のコンテンツと上記公開鍵を記録させること

を特徴とする請求項３５記載の媒体。

39. 上記プログラムは、さらに、

上記電子署名データを上記公開鍵を用い復号化し、復号化データを生成し、

上記第１の所定データを所定のアルゴリズムに基づいて第２の所定データに変換し、

上記復号化データと上記第２の所定データとを照合すること

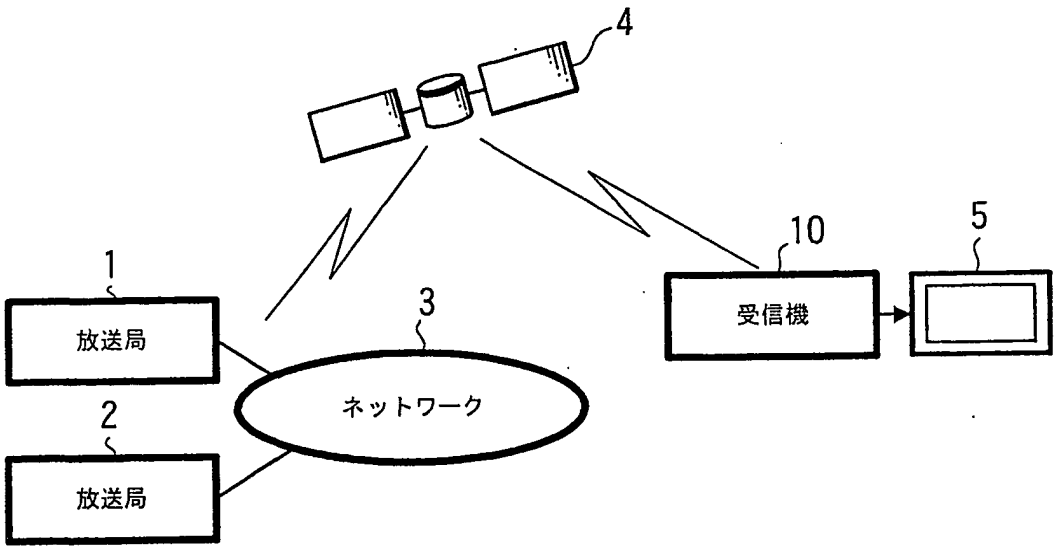
を特徴とする請求項３８記載の媒体。

40. 上記プログラムは、さらに、

上記照合の結果が一致した場合、上記第１の所定データに基づき、既に記録された第２のコンテンツを所定のタイミングで参照すること

を特徴とする請求項３９記載の媒体。

FIG. 1



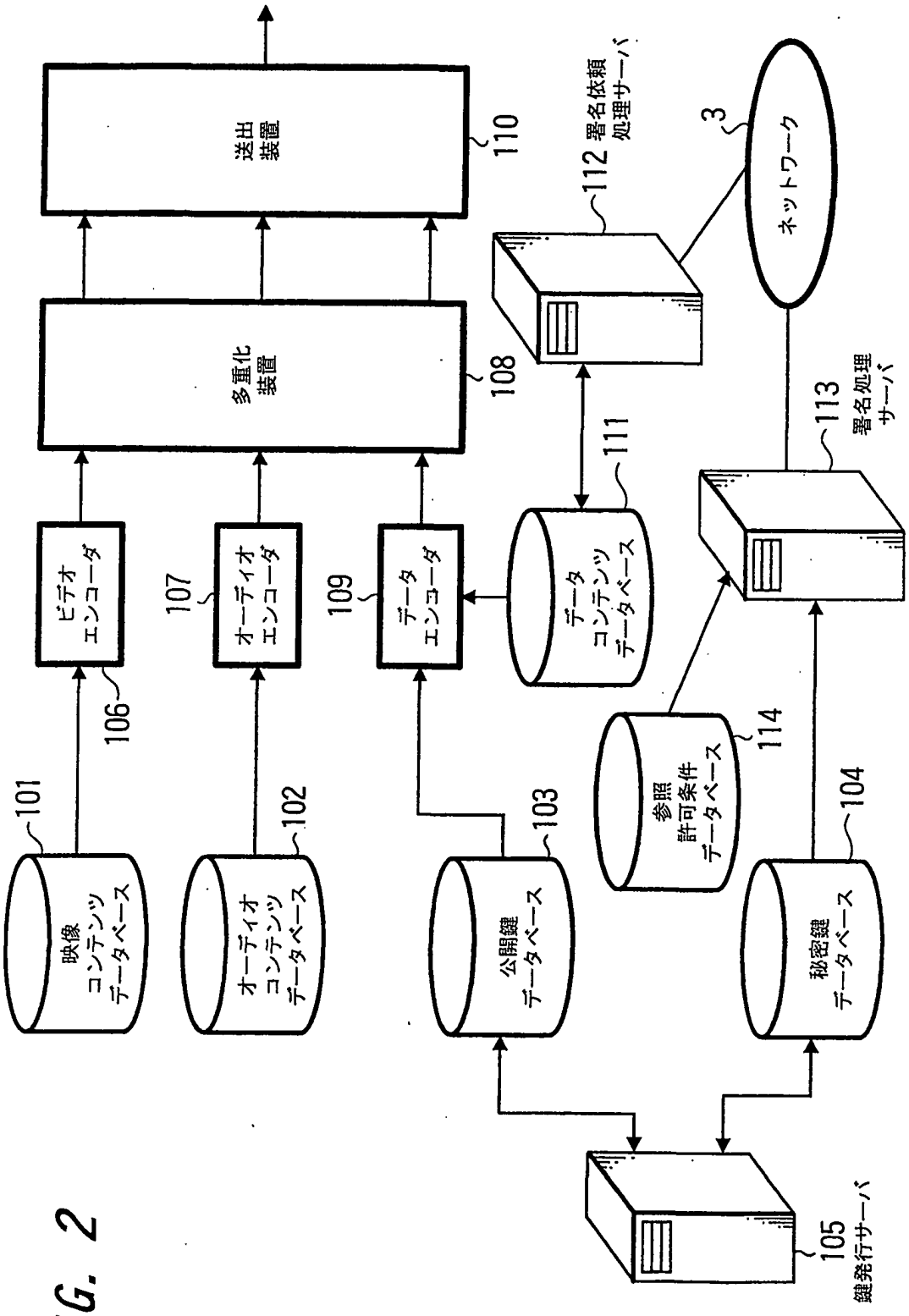
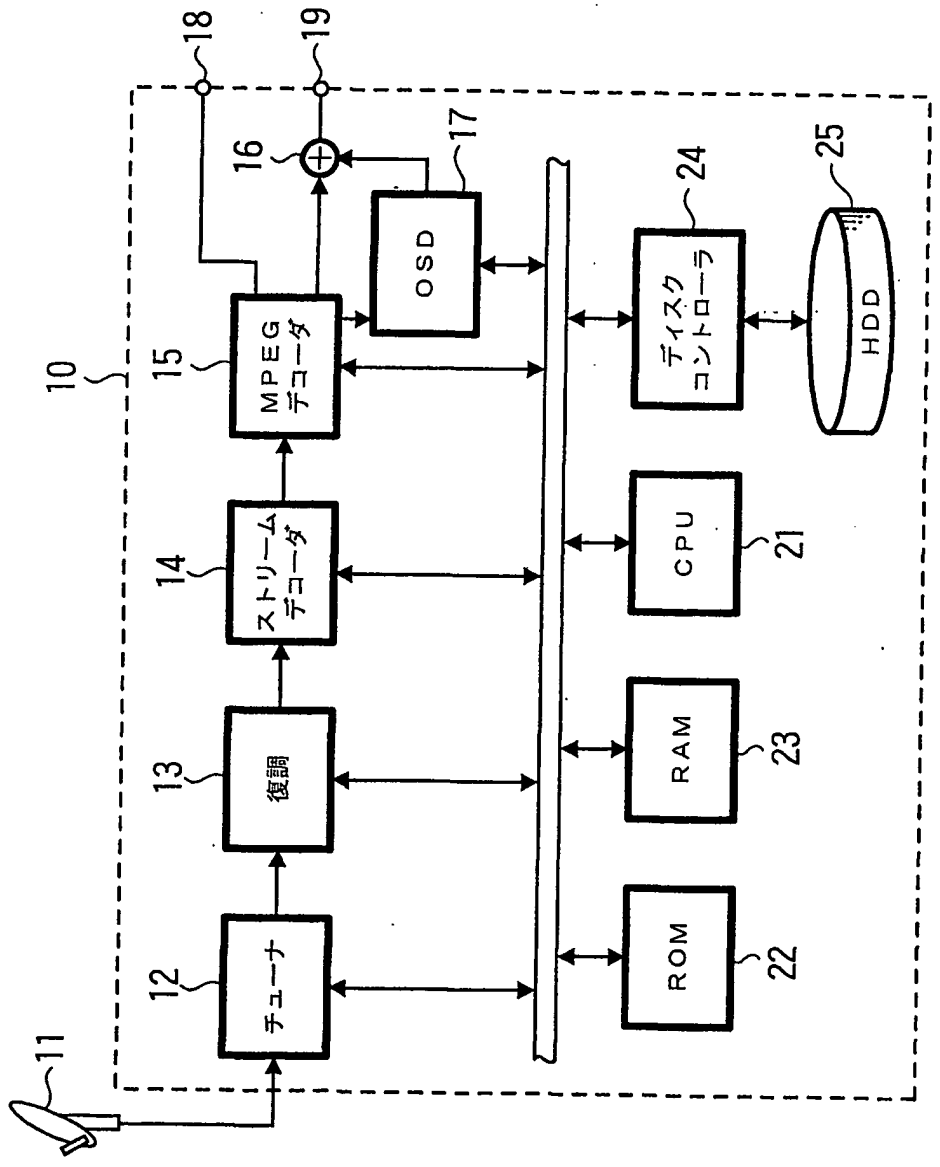

送出装置
110
多重化装置
108
ビデオエンコーダ
106
オーディオエンコーダ
107
データエンコーダ
109
映像コンテンツデータベース
101
オーディオコンテンツデータベース
102
公開鍵データベース
103
データコンテンツデータベース
111
署名依頼処理サーバ
112
ネットワーク
3
署名処理サーバ
113
参照許可条件データベース
114
秘密鍵データベース
104
鍵発行サーバ
105

FIG. 2

FIG. 3


10
11
12
チューナ
13
復調
14
ストリーム デコーダ
15
MPEG デコーダ
16
17
OSD
18
19
21
CPU
22
ROM
23
RAM
24
ディスク コントローラ
25
HDD

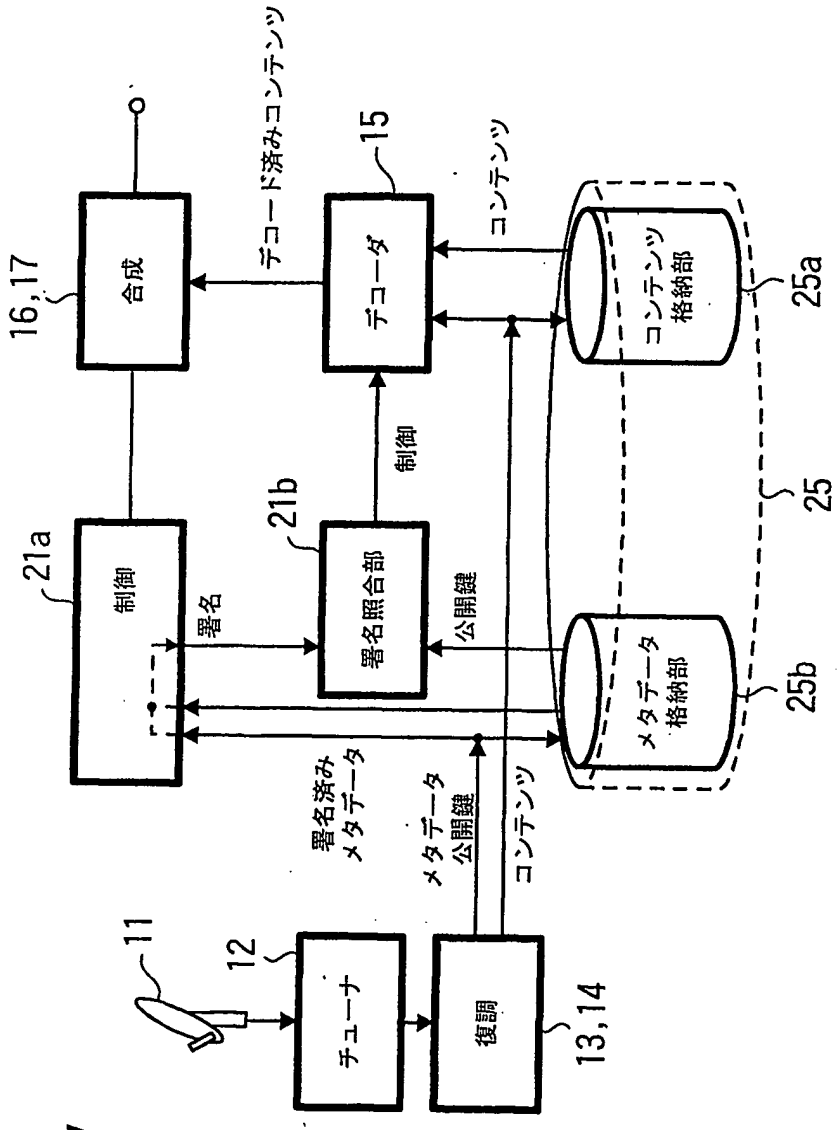

11
12
チューナ
復調
13,14
署名済み
メタデータ
メタデータ
公開鍵
コンテンツ
制御
署名
署名照合部
公開鍵
21a
21b
16,17
合成
デコード済みコンテンツ
15
デコーダ
コンテンツ
コンテンツ
格納部
25a
25
メタデータ
格納部
25b

FIG. 4

FIG. 5

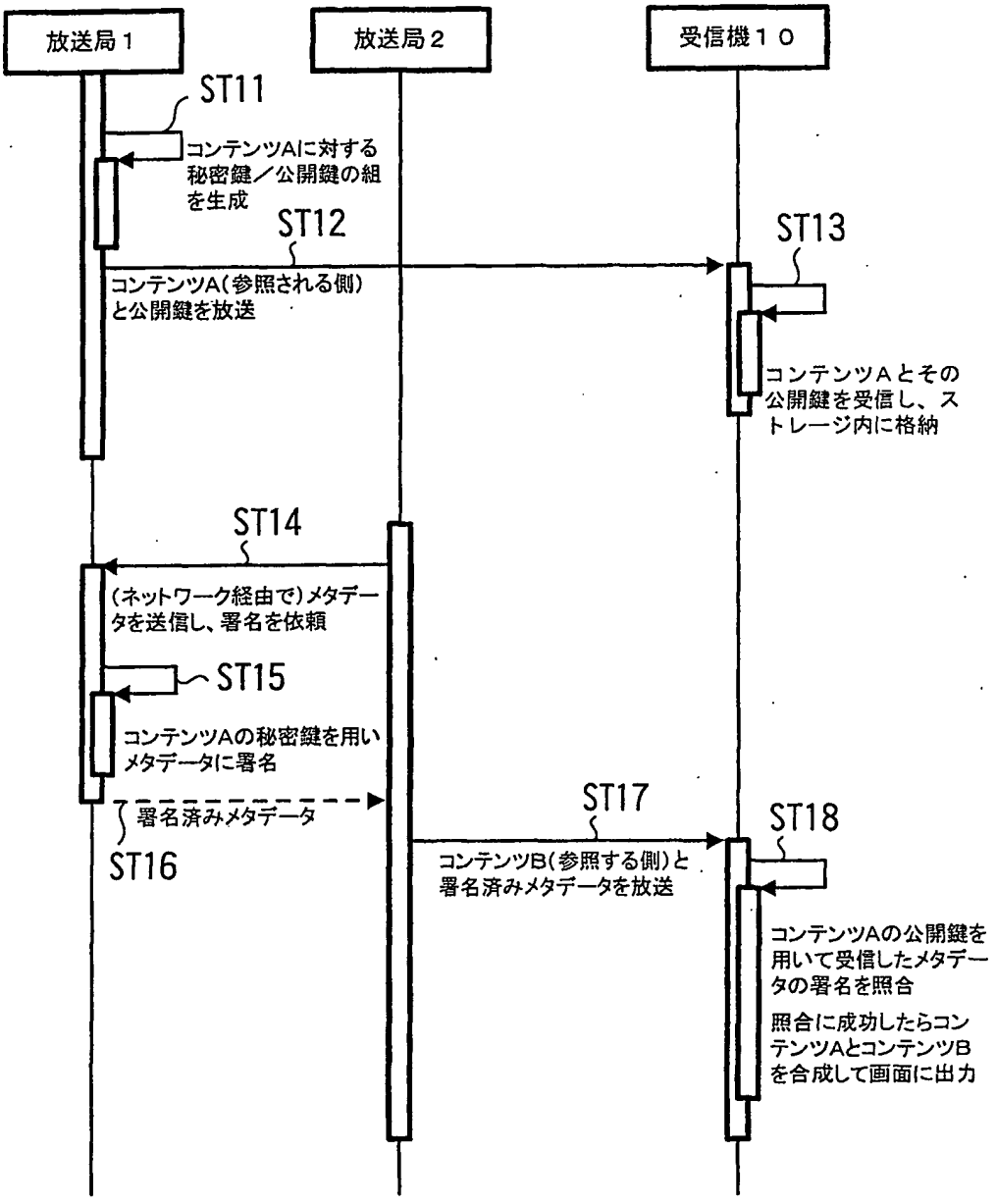

放送局１
放送局２
受信機１０
ST11
コンテンツAに対する秘密鍵／公開鍵の組を生成
ST12
ST13
コンテンツA（参照される側）と公開鍵を放送
コンテンツＡとその公開鍵を受信し、ストレージ内に格納
ST14
（ネットワーク経由で）メタデータを送信し、署名を依頼
ST15
コンテンツAの秘密鍵を用いメタデータに署名
署名済みメタデータ
ST16
ST17
ST18
コンテンツB（参照する側）と署名済みメタデータを放送
コンテンツAの公開鍵を用いて受信したメタデータの署名を照合
照合に成功したらコンテンツAとコンテンツBを合成して画面に出力

FIG. 6

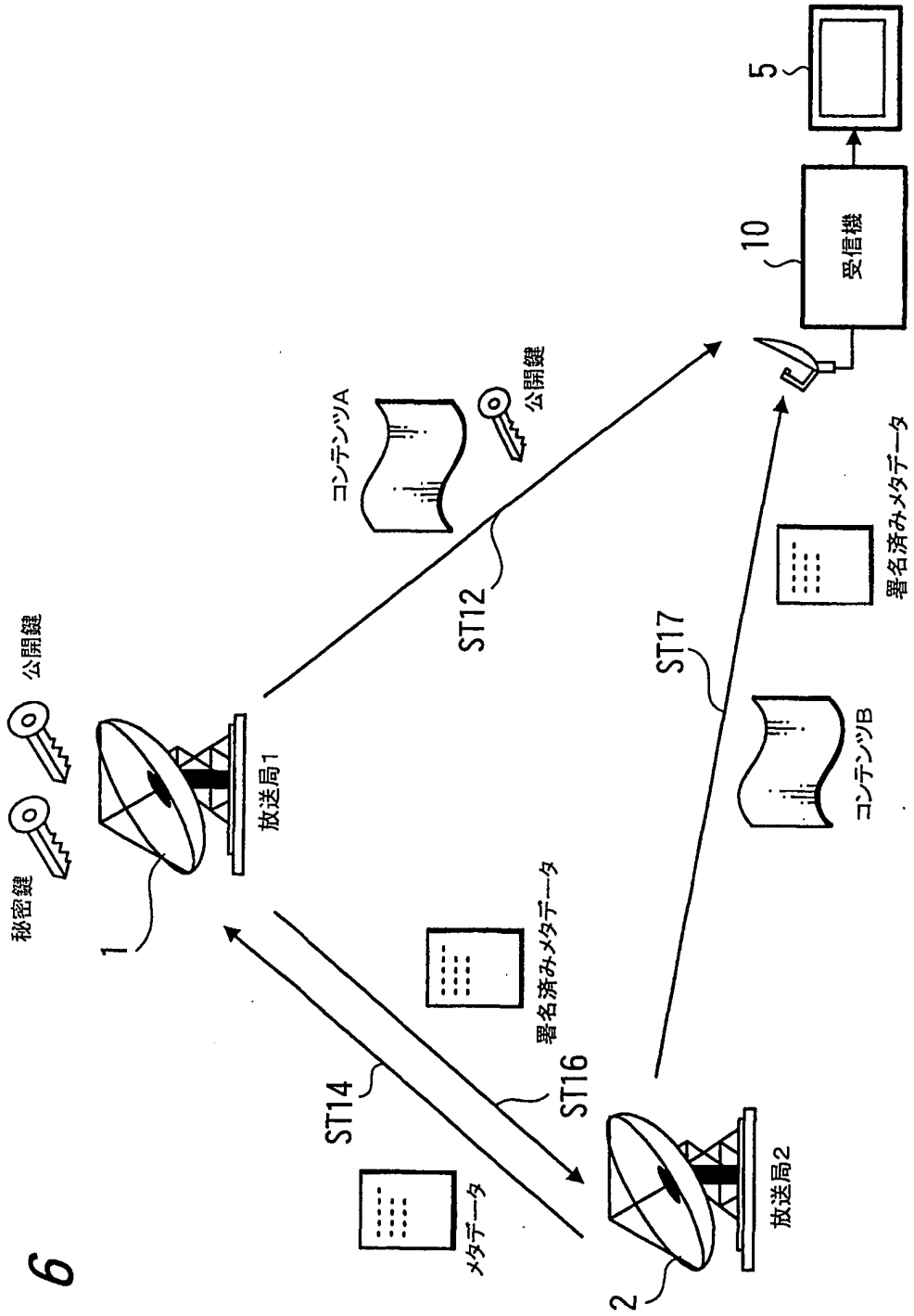

秘密鍵
公開鍵
1
放送局1
ST12
コンテンツA
公開鍵
ST14
メタデータ
署名済みメタデータ
ST16
2
放送局2
ST17
コンテンツB
署名済みメタデータ
10
受信機
5

FIG. 7

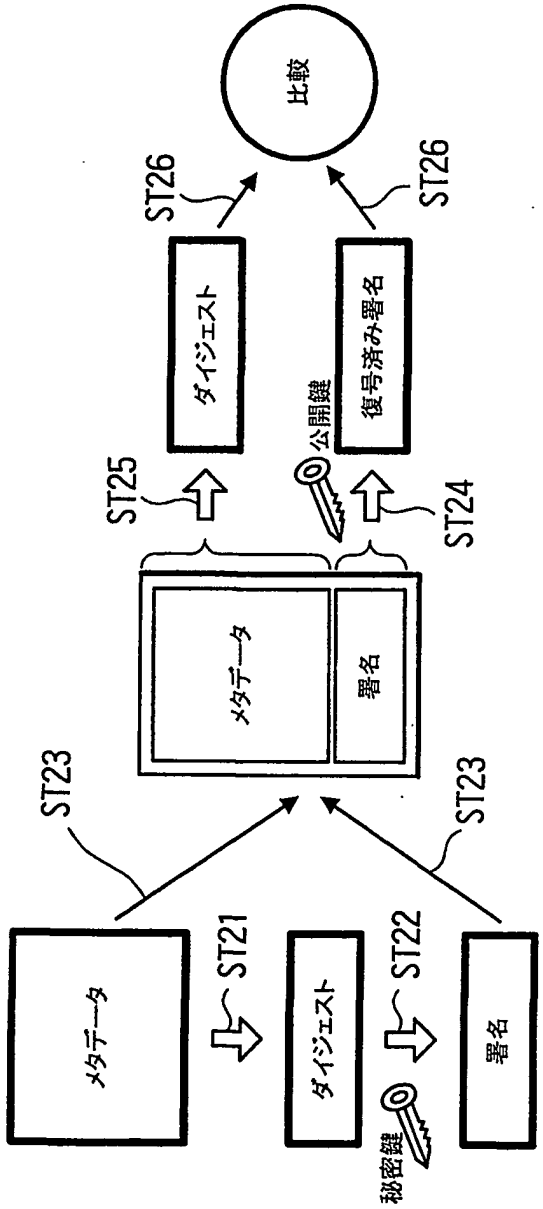

比較
ST26
ST26
ダイジェスト
復号済み署名
公開鍵
ST25
ST24
メタデータ
署名
ST23
ST23
メタデータ
ST21
ダイジェスト
ST22
署名
秘密鍵

FIG. 8

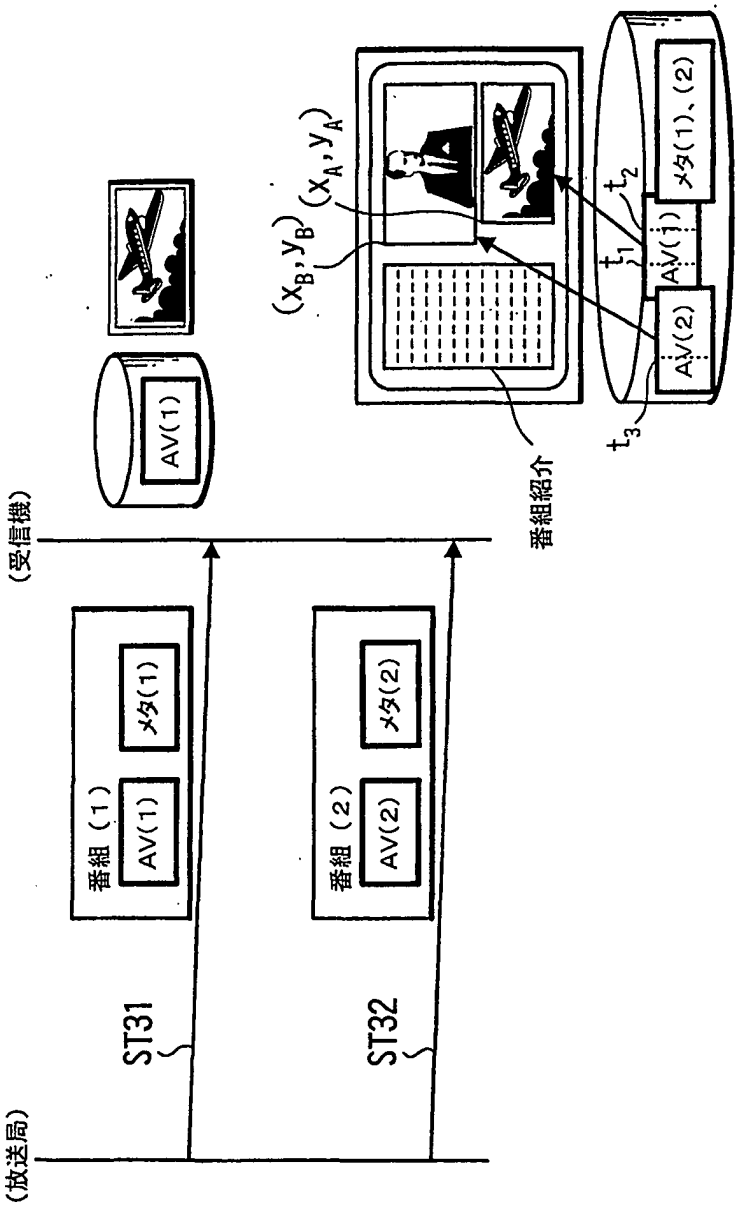
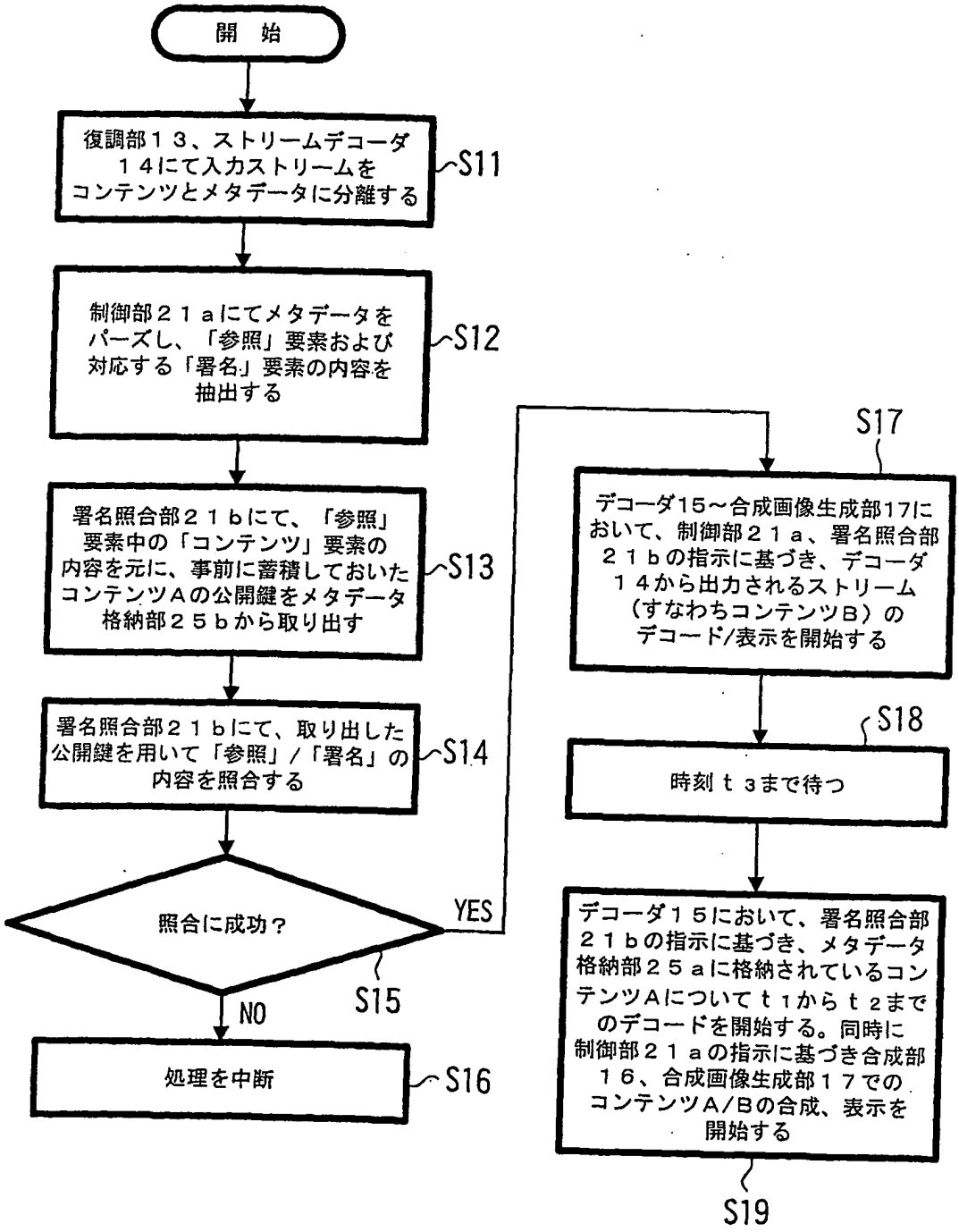

(放送局)
(受信機)
ST31
ST32
番組(1)
AV(1)
メタ(1)
番組(2)
AV(2)
メタ(2)
AV(1)
(x_B, y_B)
(x_A, y_A)
番組紹介
t_1
t_2
t_3
AV(1)
AV(2)
メタ(1)、(2)

FIG. 9


開 始
復調部１３、ストリームデコーダ１４にて入力ストリームをコンテンツとメタデータに分離する
S11
制御部２１ａにてメタデータをパーズし、「参照」要素および対応する「署名」要素の内容を抽出する
S12
署名照合部２１ｂにて、「参照」要素中の「コンテンツ」要素の内容を元に、事前に蓄積しておいたコンテンツＡの公開鍵をメタデータ格納部２５ｂから取り出す
S13
署名照合部２１ｂにて、取り出した公開鍵を用いて「参照」/「署名」の内容を照合する
S14
照合に成功？
YES
S15
NO
処理を中断
S16
S17
デコーダ15～合成画像生成部17において、制御部２１ａ、署名照合部２１ｂの指示に基づき、デコーダ１４から出力されるストリーム（すなわちコンテンツＢ）のデコード/表示を開始する
S18
時刻ｔ３まで待つ
デコーダ１５において、署名照合部２１ｂの指示に基づき、メタデータ格納部２５ａに格納されているコンテンツＡについてｔ１からｔ２までのデコードを開始する。同時に制御部２１ａの指示に基づき合成部１６、合成画像生成部１７でのコンテンツＡ/Ｂの合成、表示を開始する
S19

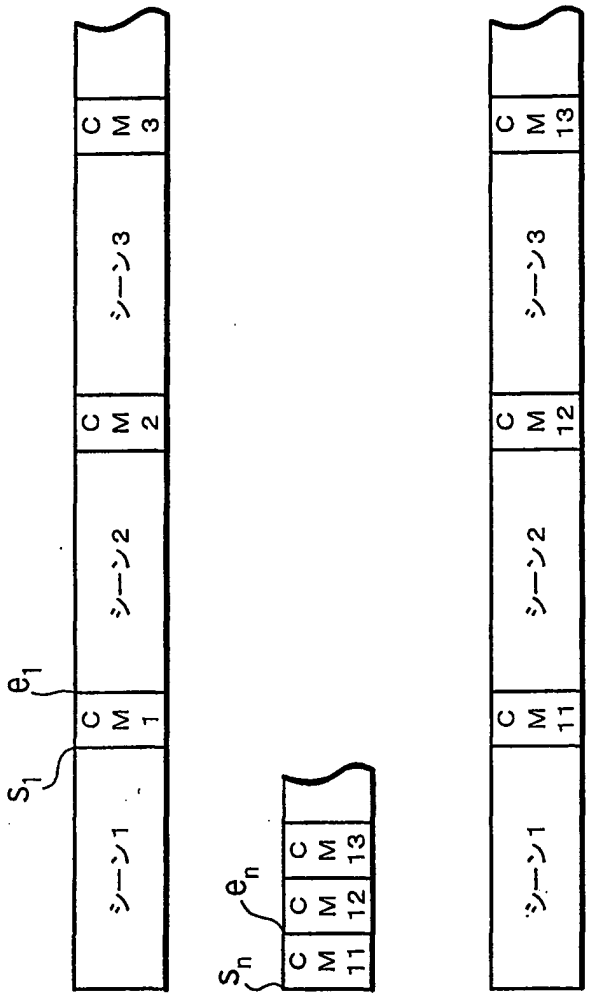


FIG. 10A

FIG. 10B

FIG. 10C

FIG. 11

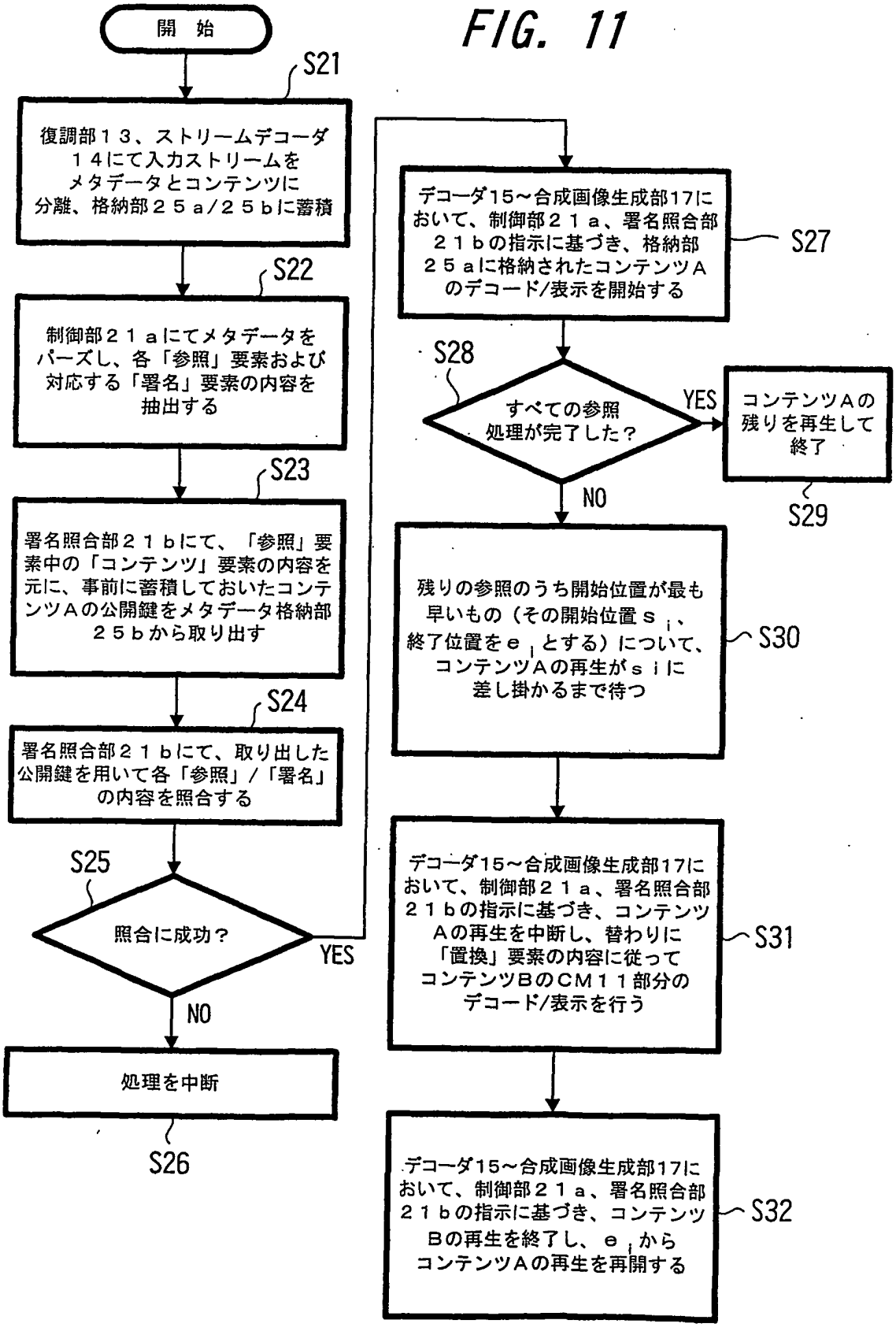
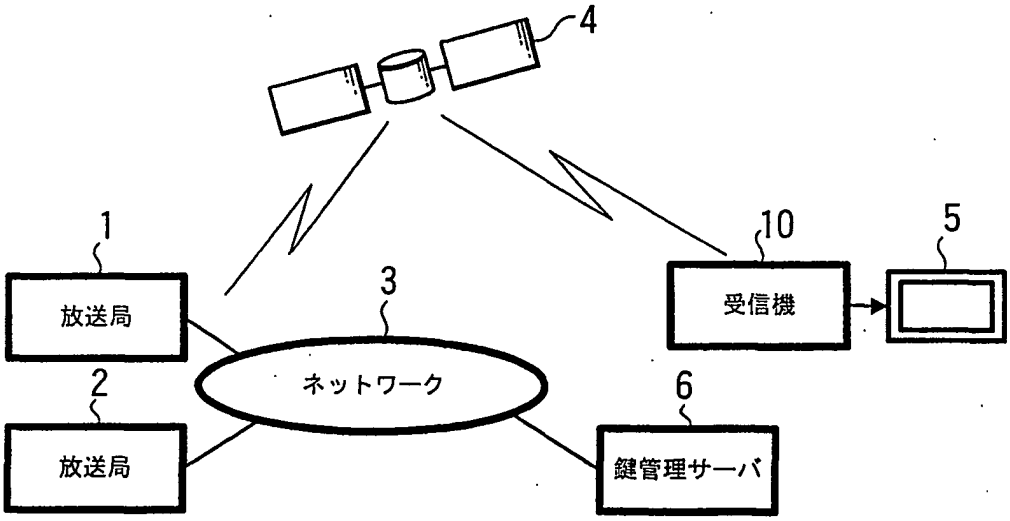

開 始
S21
復調部１３、ストリームデコーダ１４にて入力ストリームをメタデータとコンテンツに分離、格納部２５ａ/２５ｂに蓄積
S22
制御部２１ａにてメタデータをパーズし、各「参照」要素および対応する「署名」要素の内容を抽出する
S23
署名照合部２１ｂにて、「参照」要素中の「コンテンツ」要素の内容を元に、事前に蓄積しておいたコンテンツＡの公開鍵をメタデータ格納部２５ｂから取り出す
S24
署名照合部２１ｂにて、取り出した公開鍵を用いて各「参照」/「署名」の内容を照合する
S25
照合に成功？
YES
NO
処理を中断
S26
デコーダ15～合成画像生成部17において、制御部２１ａ、署名照合部２１ｂの指示に基づき、格納部２５ａに格納されたコンテンツＡのデコード/表示を開始する
S27
S28
すべての参照処理が完了した？
YES
コンテンツＡの残りを再生して終了
S29
NO
残りの参照のうち開始位置が最も早いもの（その開始位置ｓ ｉ、終了位置をｅ ｉとする）について、コンテンツＡの再生がｓｉに差し掛かるまで待つ
S30
デコーダ15～合成画像生成部17において、制御部２１ａ、署名照合部２１ｂの指示に基づき、コンテンツＡの再生を中断し、替わりに「置換」要素の内容に従ってコンテンツＢのＣＭ１１部分のデコード/表示を行う
S31
デコーダ15～合成画像生成部17において、制御部２１ａ、署名照合部２１ｂの指示に基づき、コンテンツＢの再生を終了し、ｅ ｉからコンテンツＡの再生を再開する
S32

FIG. 12



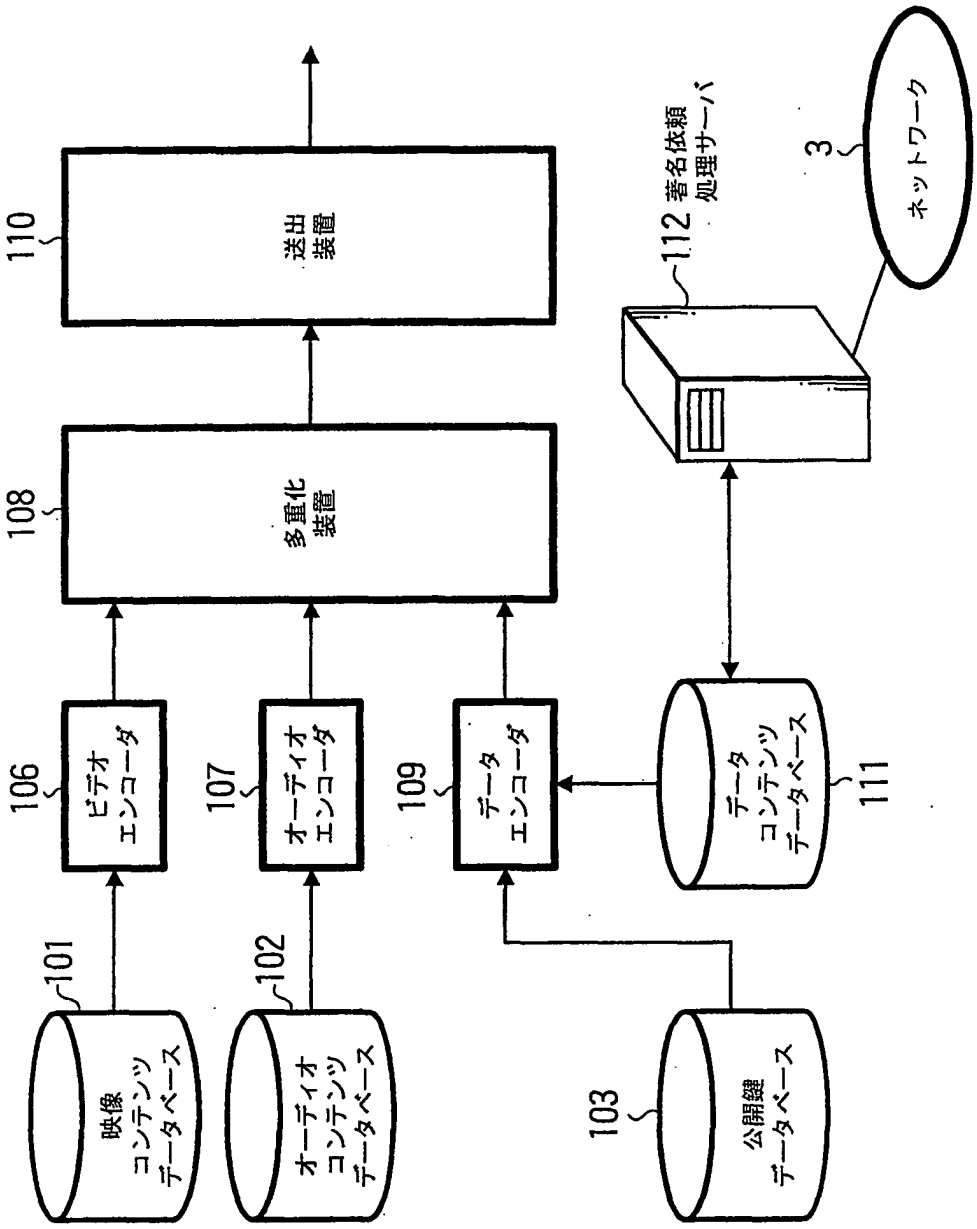

映像
コンテンツ
データベース
101
オーディオ
コンテンツ
データベース
102
公開鍵
データベース
103
ビデオ
エンコーダ
106
オーディオ
エンコーダ
107
データ
エンコーダ
109
多重化
装置
108
送出
装置
110
データ
コンテンツ
データベース
111
署名依頼
処理サーバ
112
ネットワーク
3

FIG. 13

FIG. 14

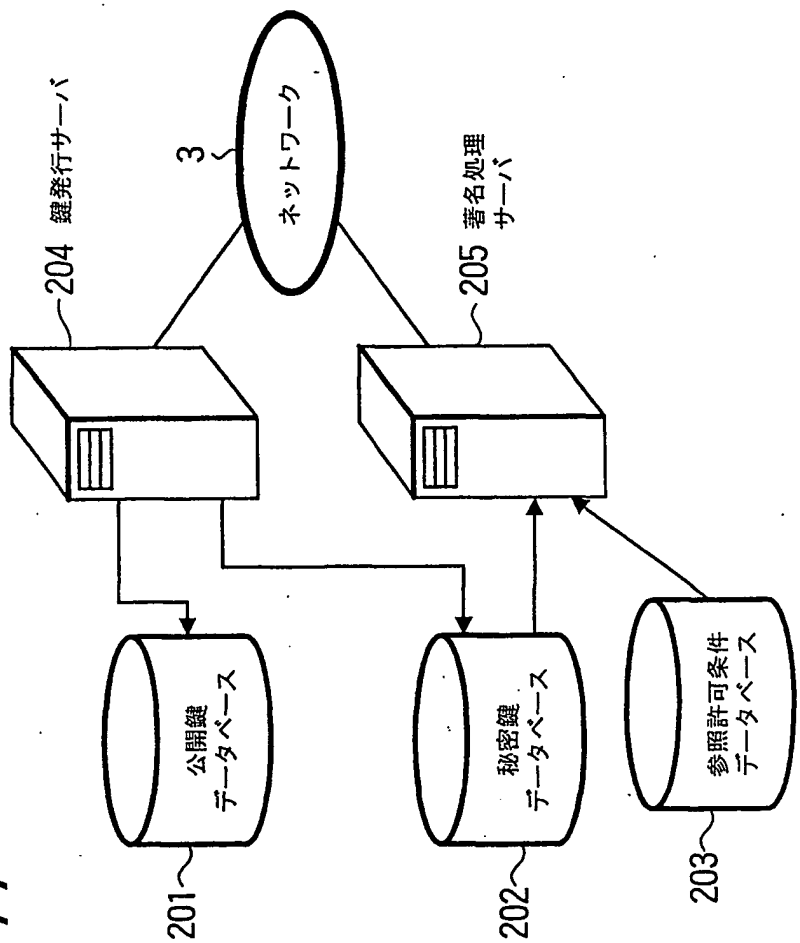

ネットワーク
3
鍵発行サーバ
204
署名処理
サーバ
205
公開鍵
データベース
201
秘密鍵
データベース
202
参照許可条件
データベース
203

FIG. 15

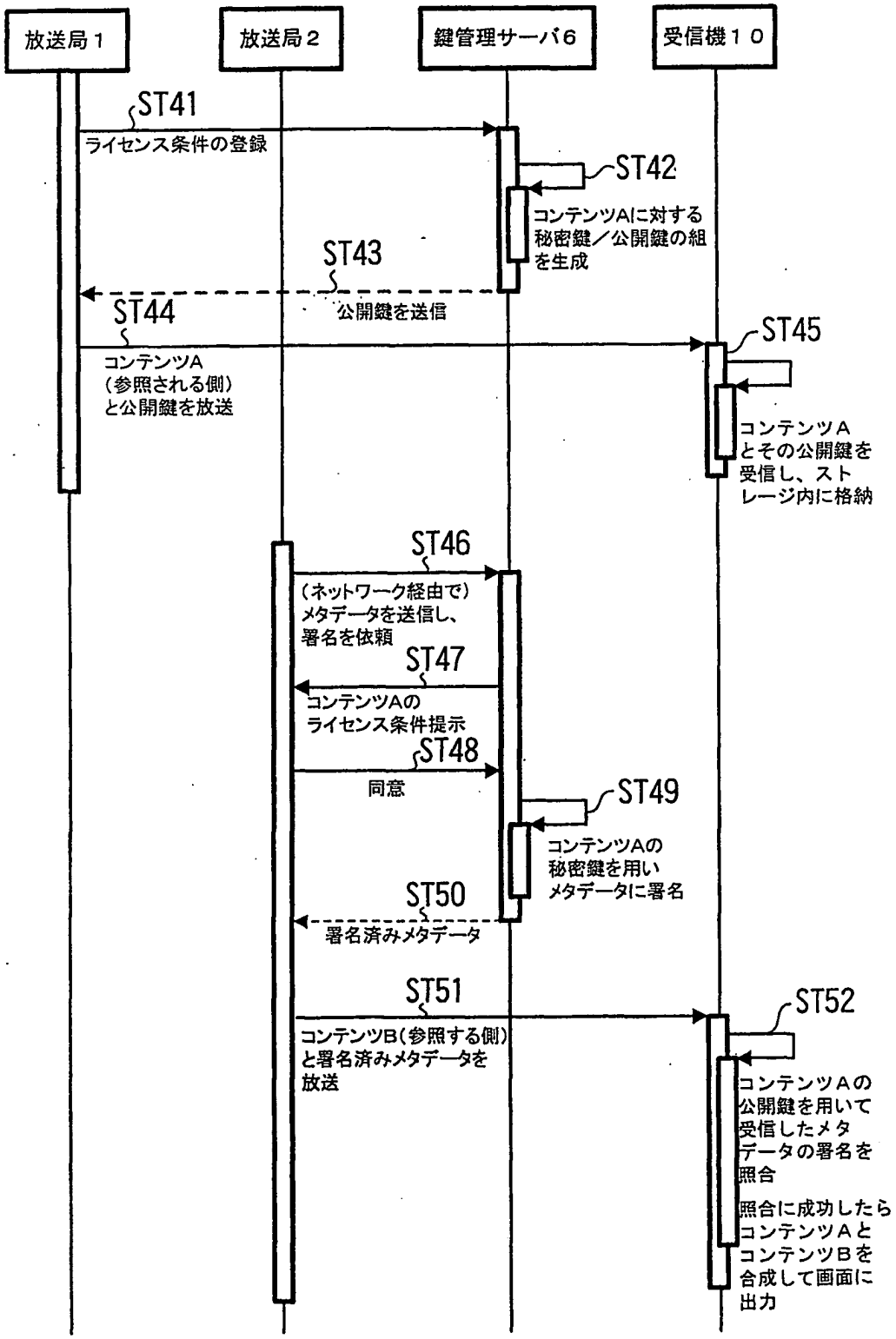
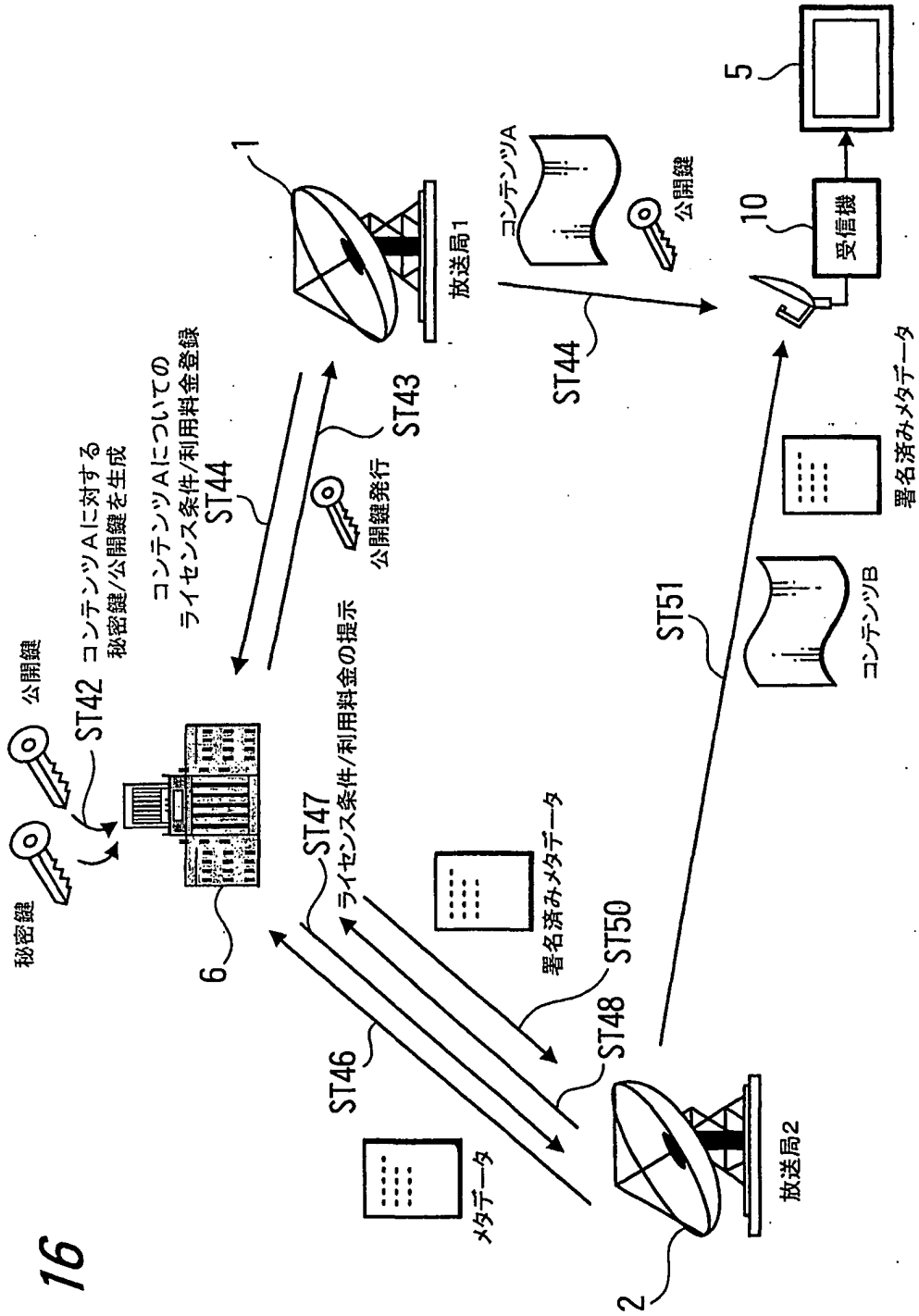

放送局１
放送局２
鍵管理サーバ６
受信機１０
ST41
ライセンス条件の登録
ST42
コンテンツAに対する
秘密鍵／公開鍵の組
を生成
ST43
公開鍵を送信
ST44
コンテンツA
（参照される側）
と公開鍵を放送
ST45
コンテンツA
とその公開鍵を
受信し、スト
レージ内に格納
ST46
（ネットワーク経由で）
メタデータを送信し、
署名を依頼
ST47
コンテンツAの
ライセンス条件提示
ST48
同意
ST49
コンテンツAの
秘密鍵を用い
メタデータに署名
ST50
署名済みメタデータ
ST51
コンテンツB（参照する側）
と署名済みメタデータを
放送
ST52
コンテンツAの
公開鍵を用いて
受信したメタ
データの署名を
照合
照合に成功したら
コンテンツAと
コンテンツBを
合成して画面に
出力

FIG. 16


秘密鍵
公開鍵
ST42
コンテンツAに対する
秘密鍵/公開鍵を生成
6
ST47
ライセンス条件/利用料金の提示
メタデータ
ST46
署名済みメタデータ
ST50
ST48
2
放送局2
ST51
コンテンツB
署名済みメタデータ
5
10
受信機
コンテンツA
公開鍵
ST44
1
放送局1
コンテンツAについての
ライセンス条件/利用料金登録
ST44
公開鍵発行
ST43

引　用　符　号　の　説　明

1　……　第１の放送局
2　……　第２の放送局
3　……　ネットワーク
4　……　人工衛星
5　……　受像機
6　……　鍵管理サーバ
１０　……　受信機
１１　……　アンテナ
１２　……　チューナ部
１３　……　復調部
１４　……　ストリームデコーダ
１５　……　ＭＰＥＧデコーダ
１６　……　合成部
１７　……　合成画像生成部
１８　……　音声出力部
１９　……　映像出力部
２１　……　中央制御ユニット（ＣＰＵ）
２１ａ……　制御部
２１ｂ……　署名照合部
２２　……　ＲＯＭ
２３　……　ＲＡＭ
２４　……　ディスクコントローラ
２５　……　ハードディスクドライブ（ＨＤＤ）
２５ａ……　コンテンツ格納部
２５ｂ……　メタデータ格納部
１０１　……　映像コンテンツデータベース
１０２　……　オーディオコンテンツデータベース

１０３ …… 公開鍵データベース
１０４ …… 秘密鍵データベース
１０５ …… 鍵発行サーバ
１０６ …… ビデオエンコーダ
１０７ …… オーディオエンコーダ
１０８ …… 多重化装置
１０９ …… データエンコーダ
１１０ …… 送出装置
１１１ …… データコンテンツデータベース
１１２ …… 署名依頼処理サーバ
１１３ …… 署名処理サーバ
２０１ …… 公開鍵データベース
２０２ …… 秘密鍵データベース
２０３ …… 参照許可条件データベース
２０４ …… 鍵発行サーバ
２０５ …… 署名処理サーバ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/07924

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04N7/10, 7/16-7/173, G06F15/00-15/00, 390

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-155735 A (Mitsubishi Electric Corporation), 06 June, 2000 (06.06.00), Full text; Figs. 7 to 8 (Family: none)	1-40
Y A	JP 10-13811 A (Matsushita Electric Ind. Co., Ltd.), 16 January, 1998 (16.01.98), Full text; Figs. 1 to 70 & EP 817105 A2 & US 6035304 A	1-6,11-40 7-10
Y A	JP 11-96064 A (Nippon Telegr. & Teleph. Corp. <NTT>), 09 April, 1999 (09.04.99), Full text; Figs. 1 to 9 (Family: none)	5,6,12,13,21, 22,24,25,33, 34,36,37 1-4,7-11, 14-20,23, 26-32,35,38-40
Y A	JP 10-290443 A (Nippon Telegr. & Teleph. Corp. <NTT>), 27 October, 1998 (27.10.98), Full text; Figs. 1 to 11 (Family: none)	7-10 1-6,11-40

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
10 December, 2001 (10.12.01)

Date of mailing of the international search report
18 December, 2001 (18.12.01)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/07924

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 8-340525 A (Toshiba Corporation), 24 December, 1996 (24.12.96), Full text; Figs. 1 to 5 (Family: none)	7-10 1-6,11-40
A	JP 11-212462 A (Canon Inc.), 06 August, 1999 (06.08.99), Full text; Figs. 1 to 16 & EP 932298 A2 & CN 1239378 A	1-40

国際調査報告

国際出願番号　PCT／JP01／07924

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04N7／16

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04N7／10, 7／16－7／173, G06F15／00－15／00, 390

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2001年
日本国登録実用新案公報　1994－2001年
日本国実用新案登録公報　1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP. 2000－155735 A（三菱電機株式会社）6. 6月. 2000（06. 06. 00）全頁, 第7－8図（ファミリーなし）	1-40
Y A	JP 10－13811. A（松下電器産業株式会社）16. 1月. 1998（16. 01. 98）全頁, 第1－7図 &EP 817105 A2　&US 6035304. A	1-6, 11-40 7-10

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
10. 12. 01	18.12.01

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）
古川　哲也　5P　9746

電話番号　03－3581－1101　内線　3581

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０７９２４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名．及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ Ａ	ＪＰ　１１－９６０６４　Ａ（日本電信電話株式会社）９．４月．１９９９（０９．０４．９９）全頁，第１－９図 （ファミリーなし）	5, 6, 12, 13, 21, 22, 24, 25, 33, 34, 36, 37 1-4, 7-11, 14-20, 23, 26-32, 35, 38-40
Ｙ Ａ	ＪＰ　１０－２９０４４３　Ａ（日本電信電話株式会社）２７．１０月．１９９８（２７．１０．９８）全頁，第１－１１図 （ファミリーなし）	7-10 1-6, 11-40
Ｙ Ａ	ＪＰ．８－３４０５２５．Ａ（株式会社東芝）２４．１２月．１９９６（２４．１２．９６）全頁，第１－５図 （ファミリーなし）	7-10 1-6, 11-40
Ａ	ＪＰ　１１－２１２４６２　Ａ（キヤノン株式会社）６．８月．１９９９（０６．０８．９９）全頁，第１－１６図 ＆ＥＰ．９３２２９８　Ａ２　＆ＣＮ　１２３９３７８．Ａ	1-40

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（１９９８年７月）